

Fig. 1A
(Prior Art)

100

AGP
108

LPC BUS
118

BIOS
122

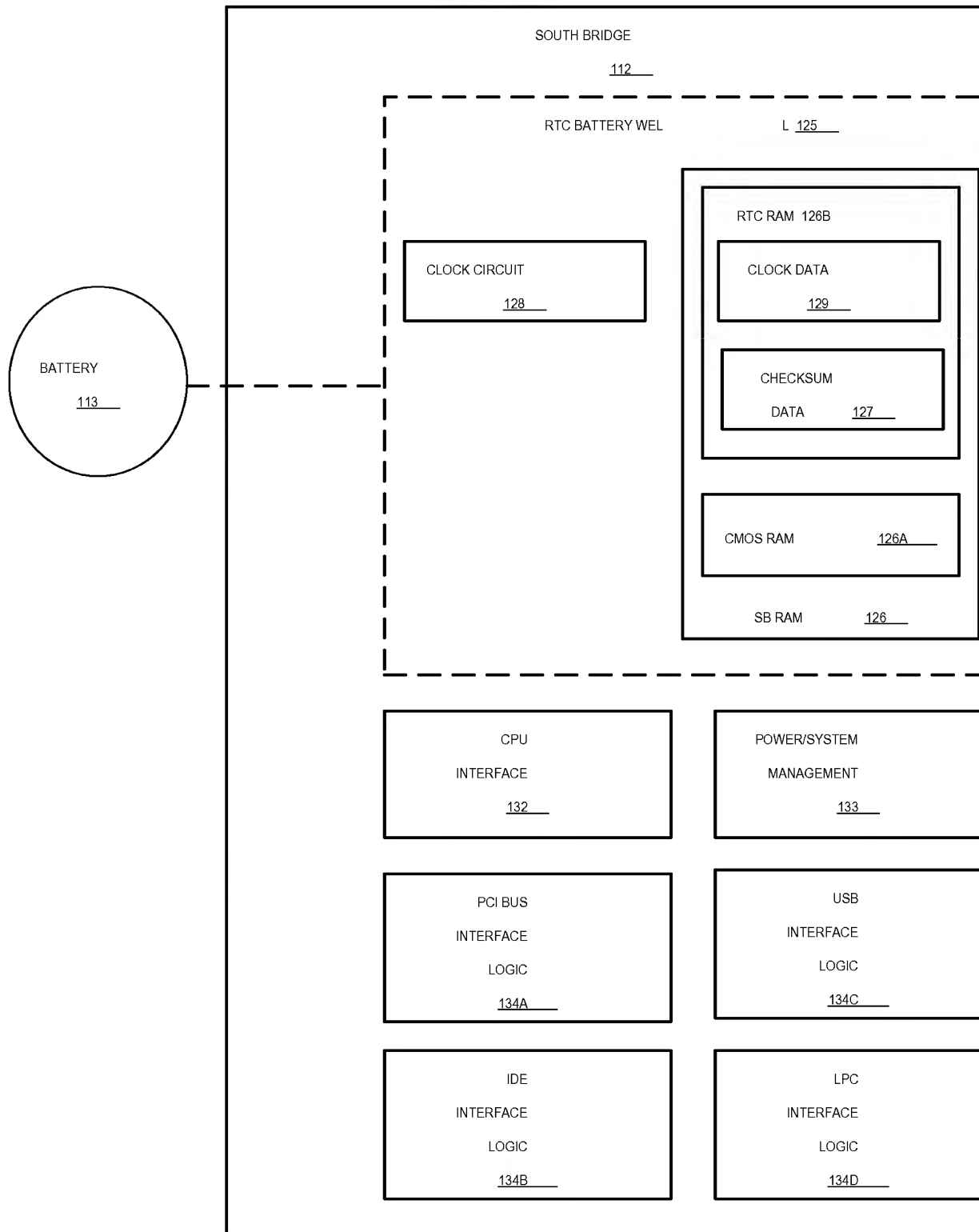
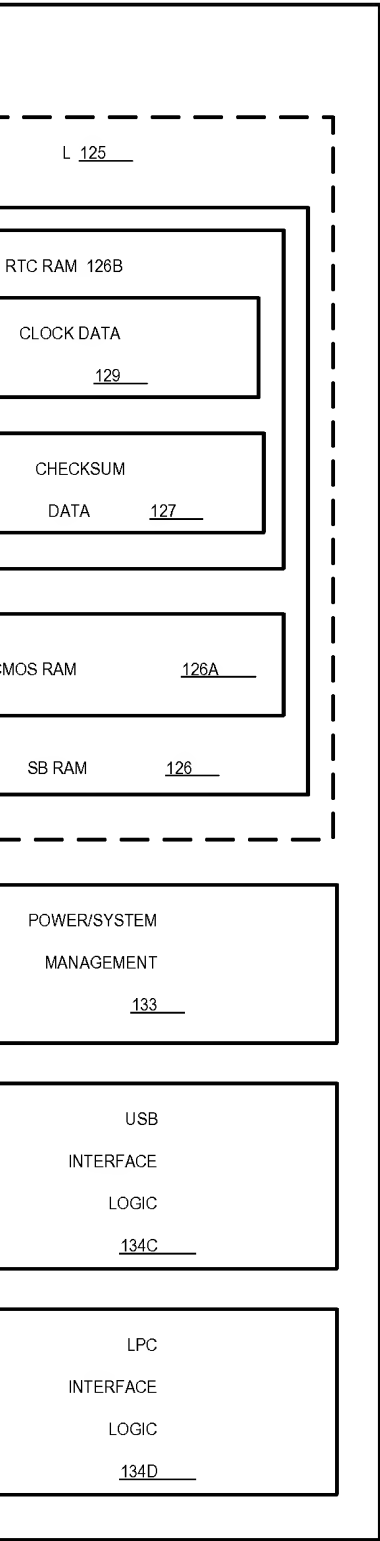


Fig. 1B
(Prior Art)



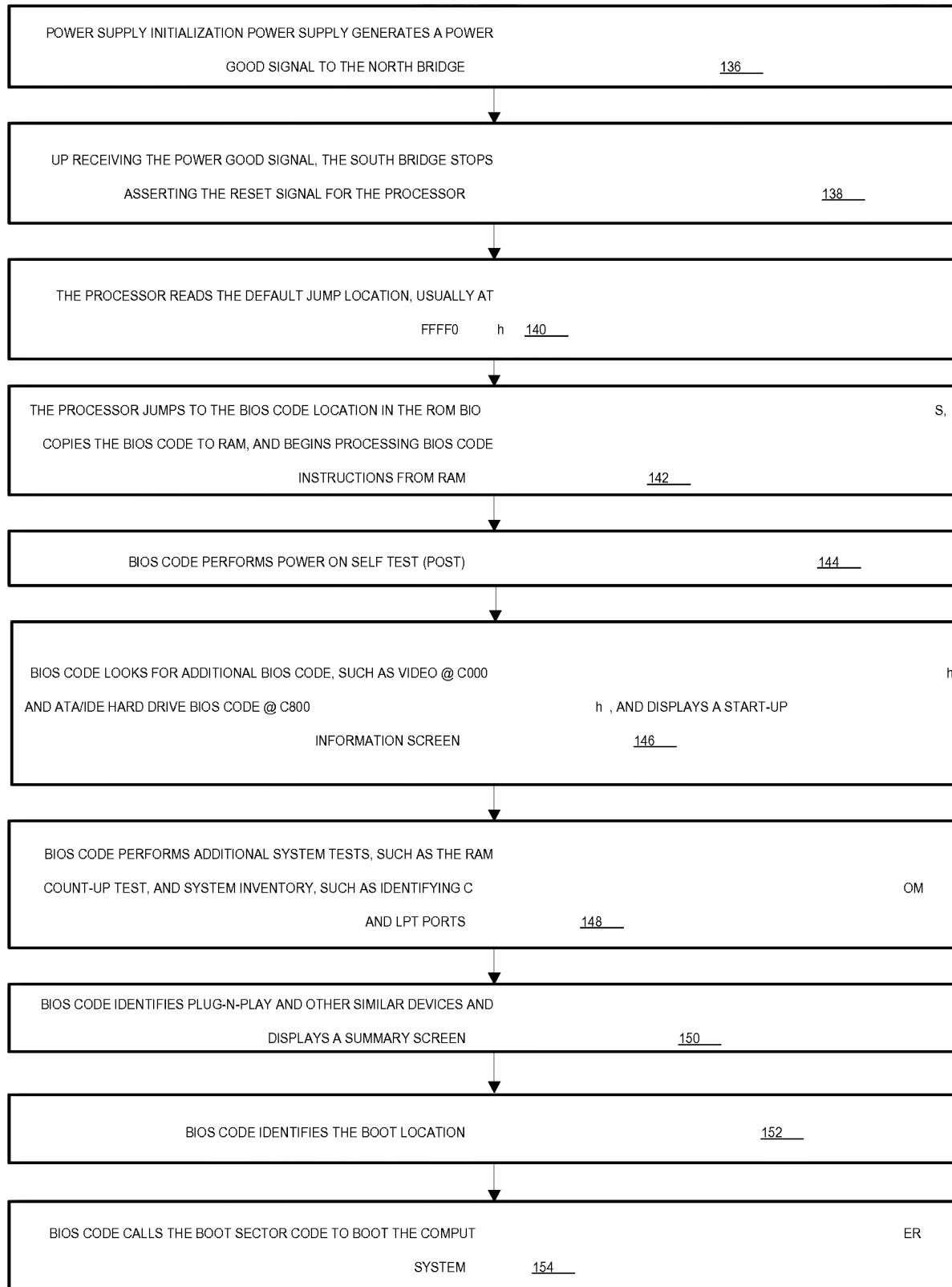


Fig. 2A

(Prior Art)

135

136

138

S,

144

h

A START-UP

OM

152

ER

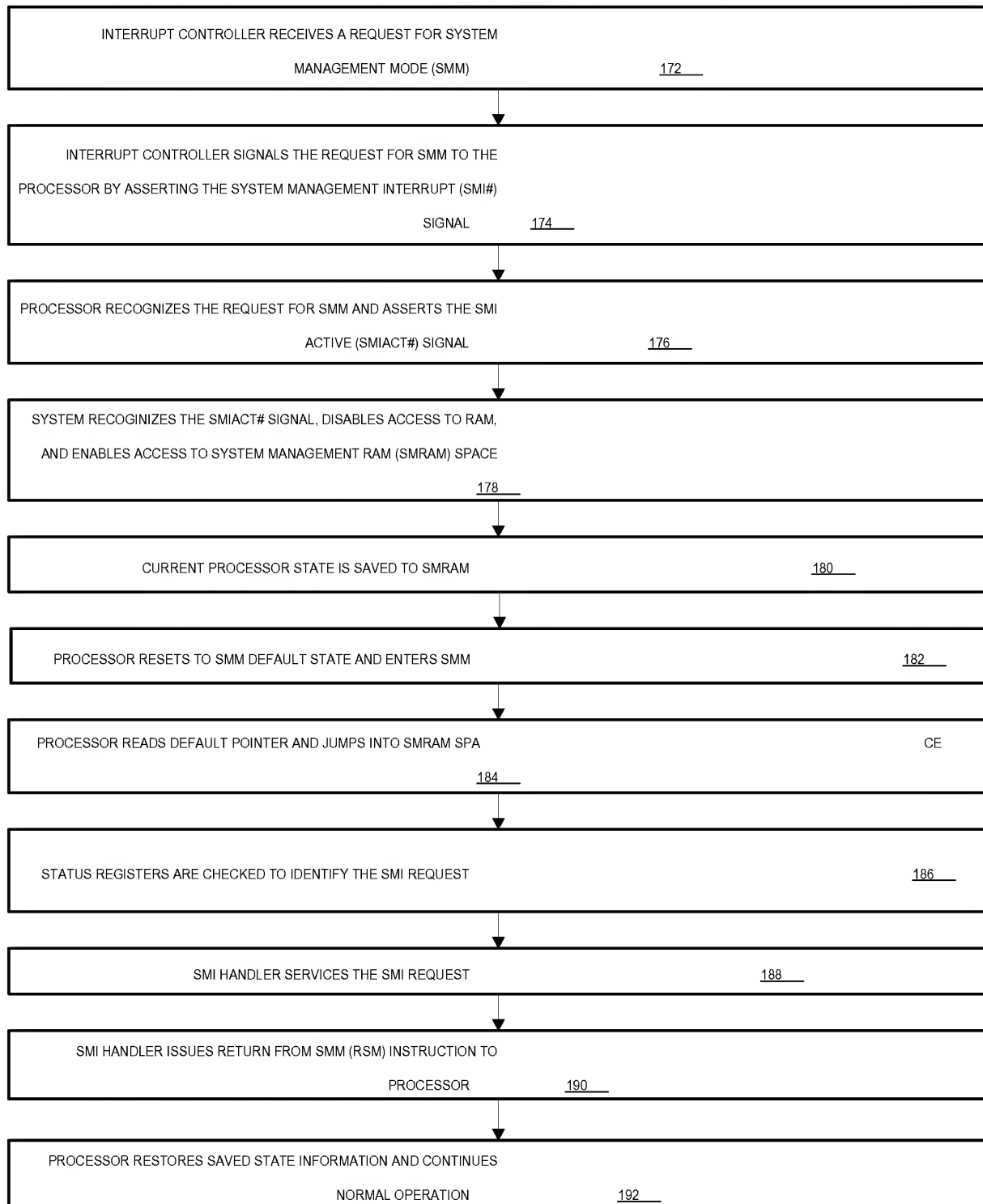


Fig. 2B

(Prior Art)

170
↙

--

--

--

--

180

182

CE

186

188

--

--

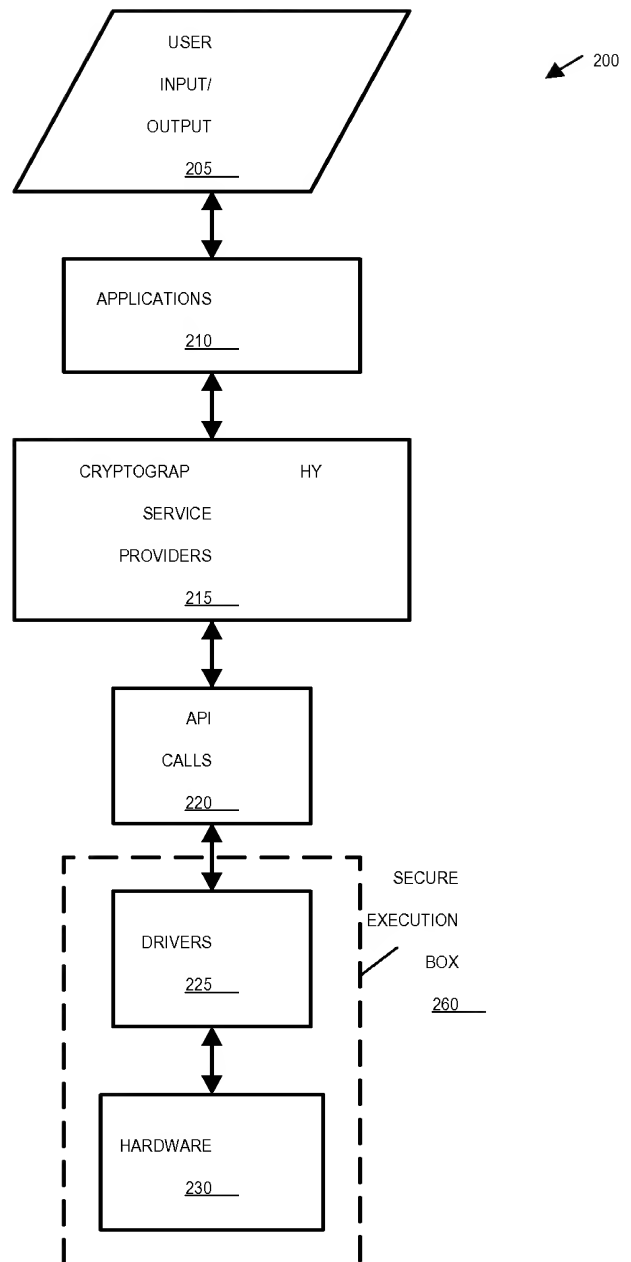


Fig. 3

200

Fig. 3

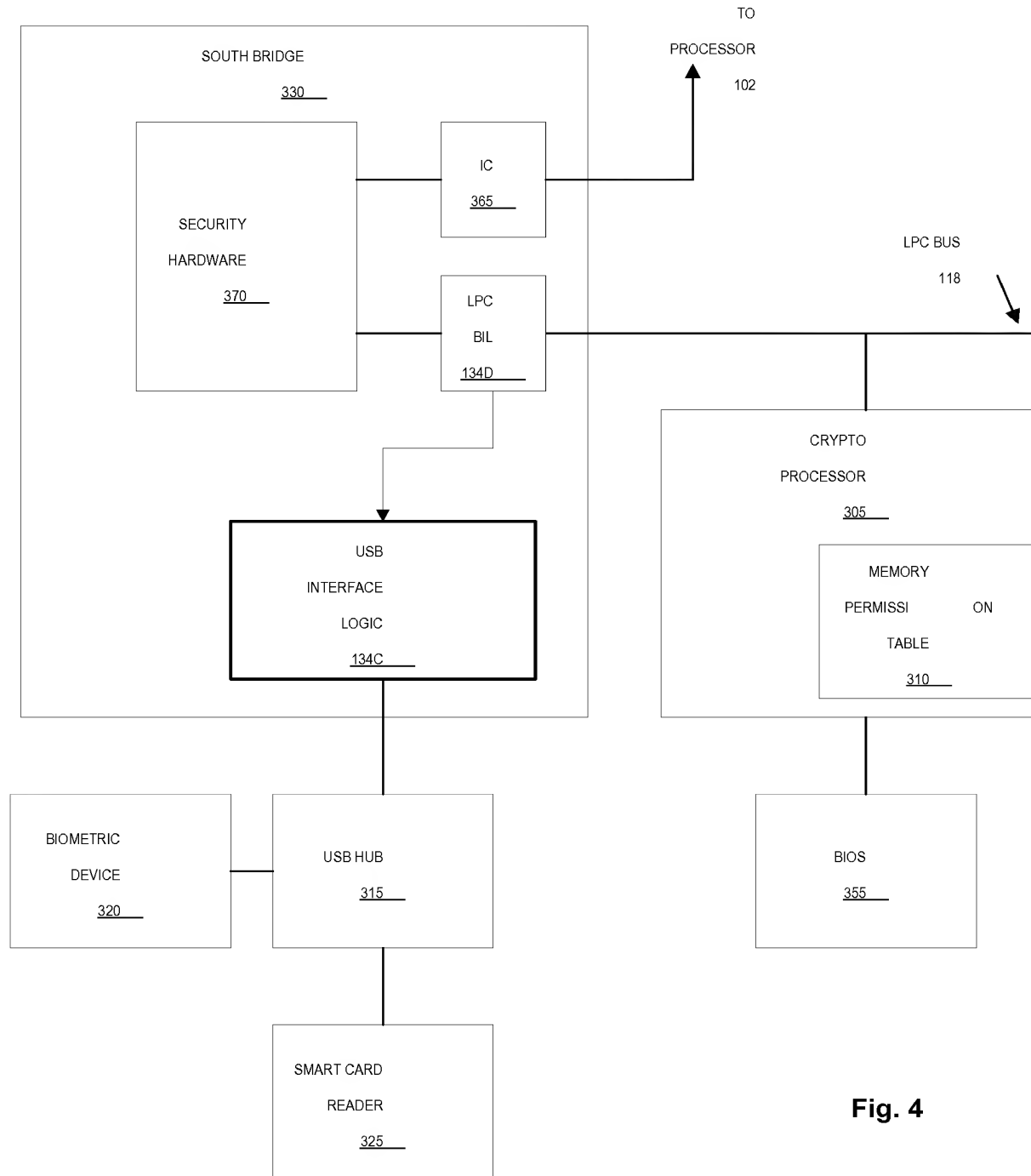


Fig. 4

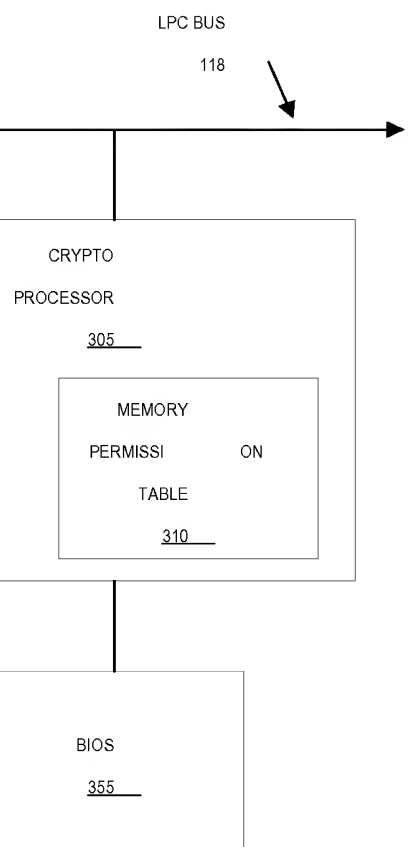


Fig. 4

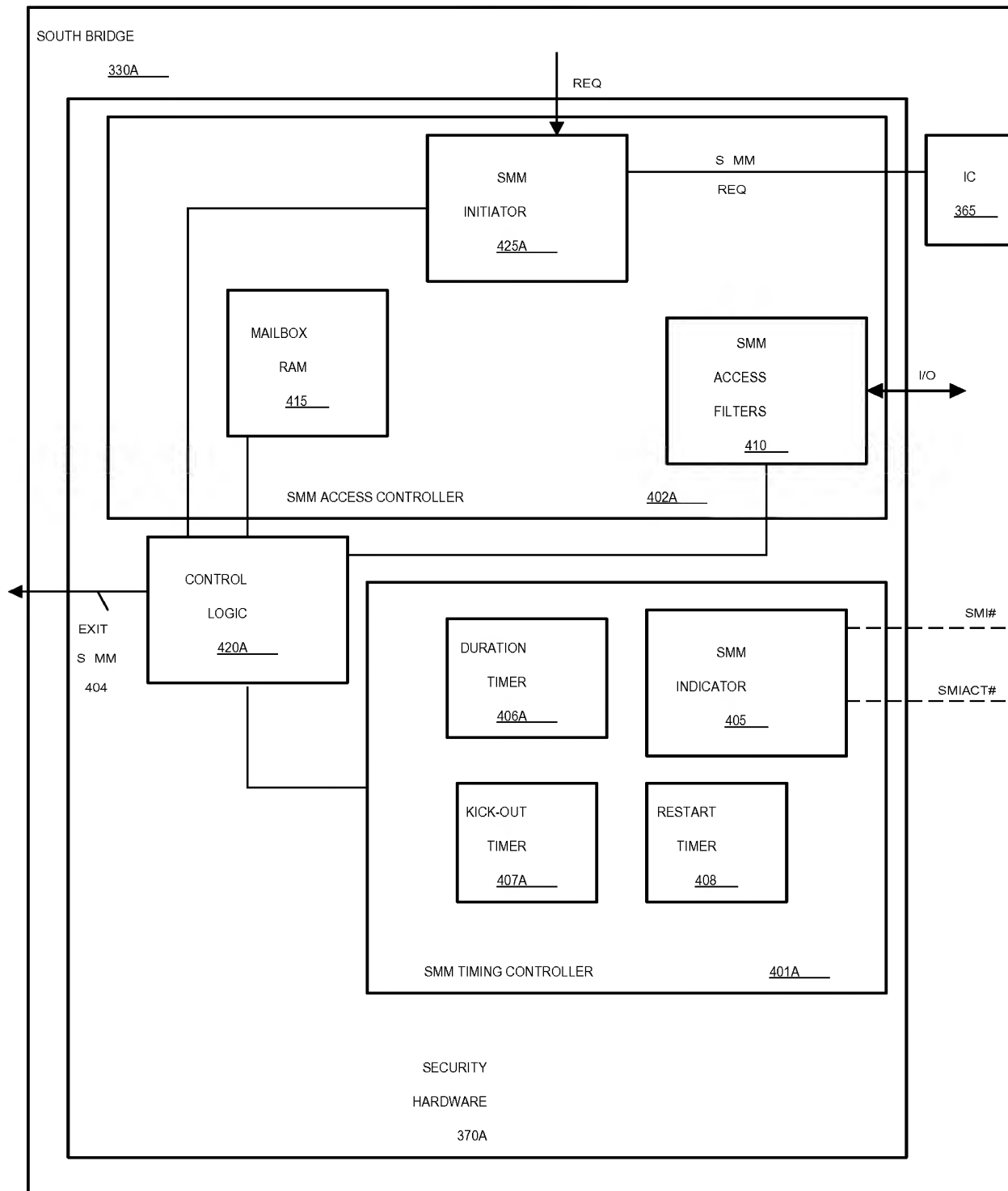
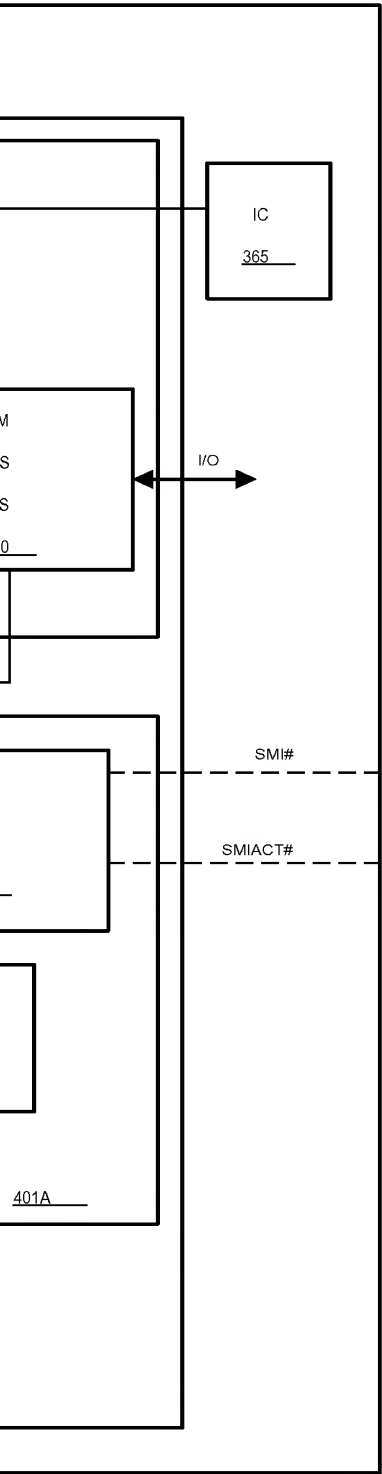


Fig. 5A



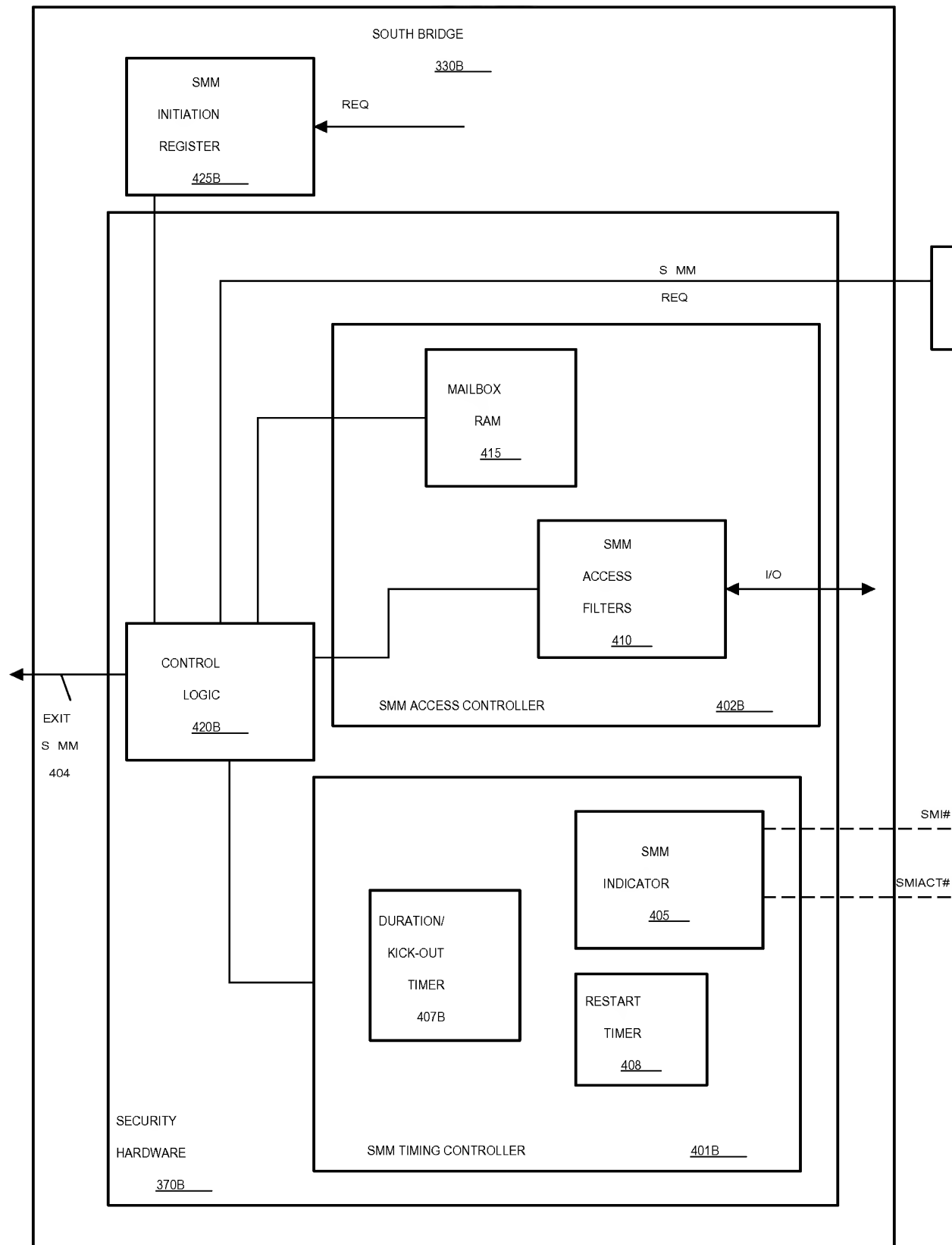
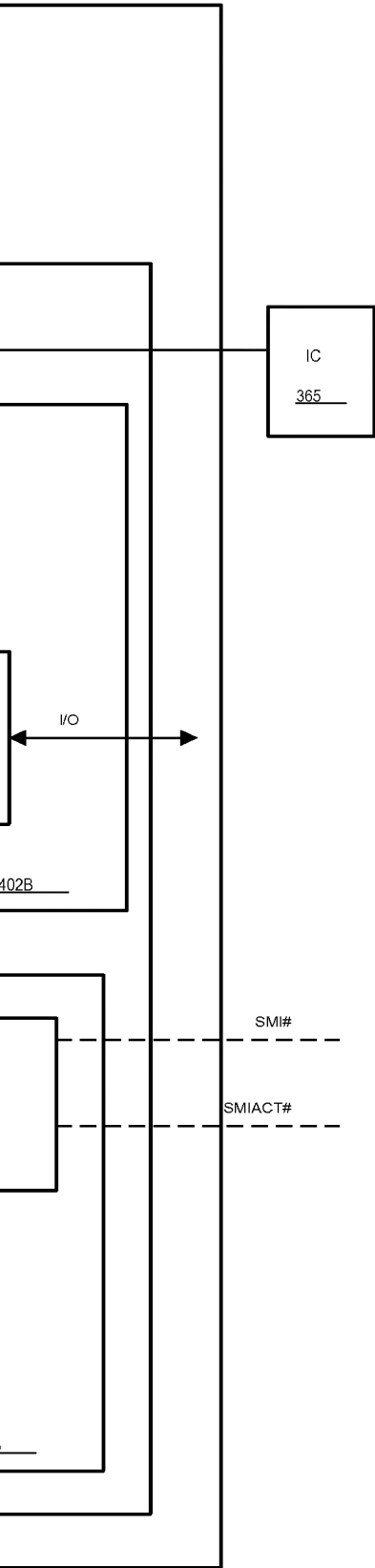


Fig. 5B



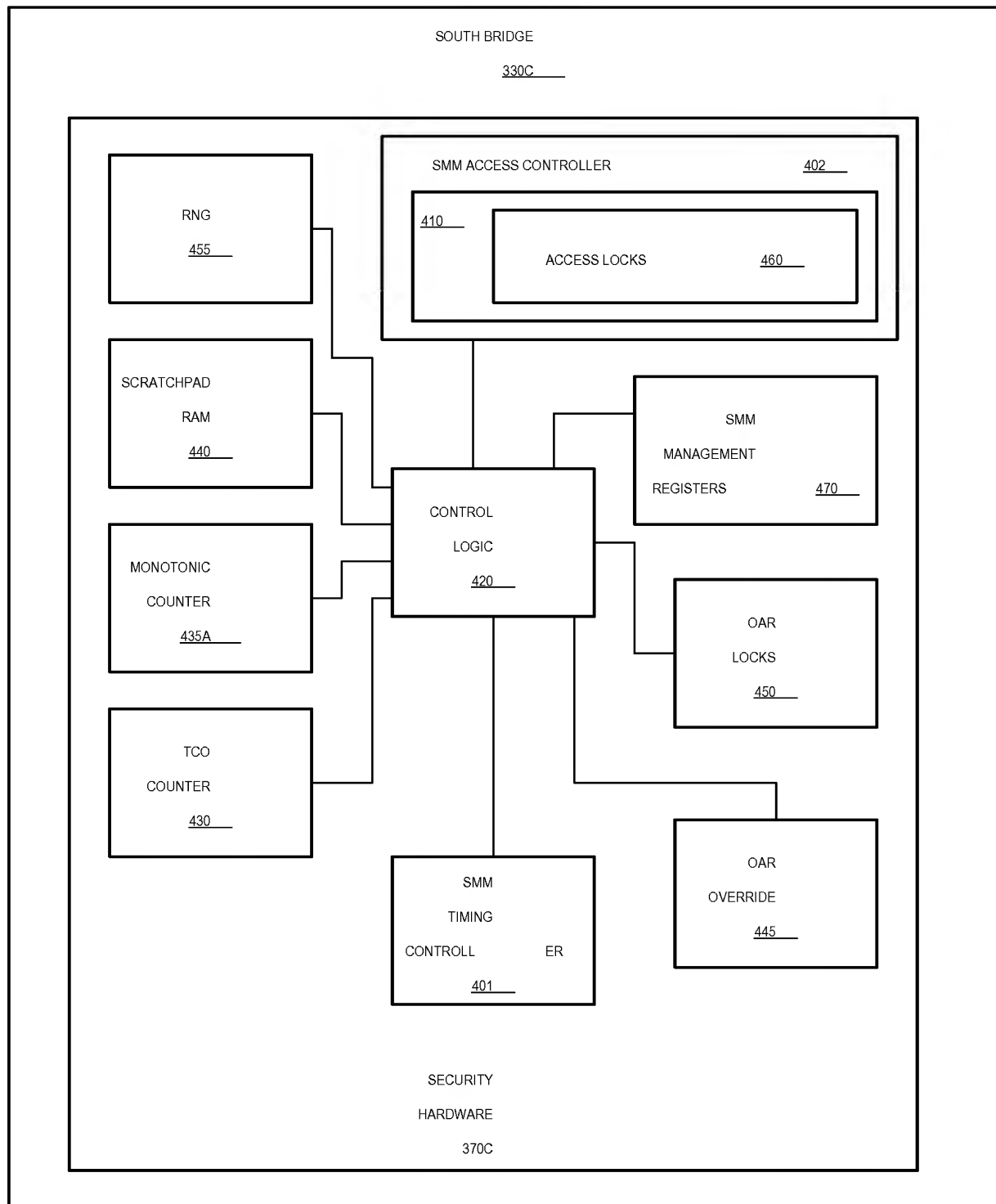


Fig. 6

402

460

M
T

470

OAR
CKS

450

OAR
RIDE

445

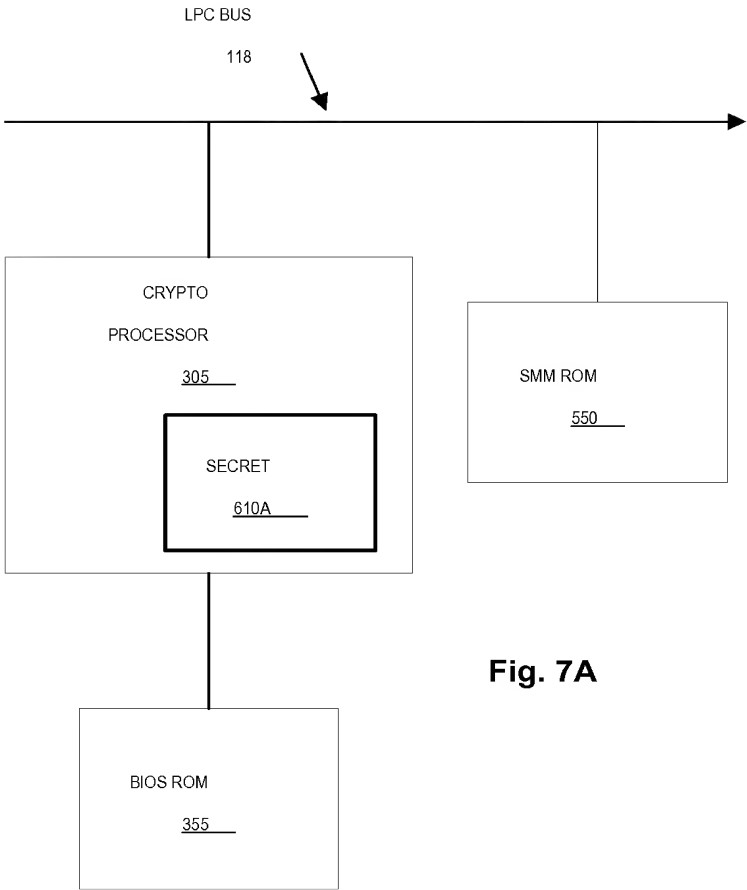


Fig. 7A

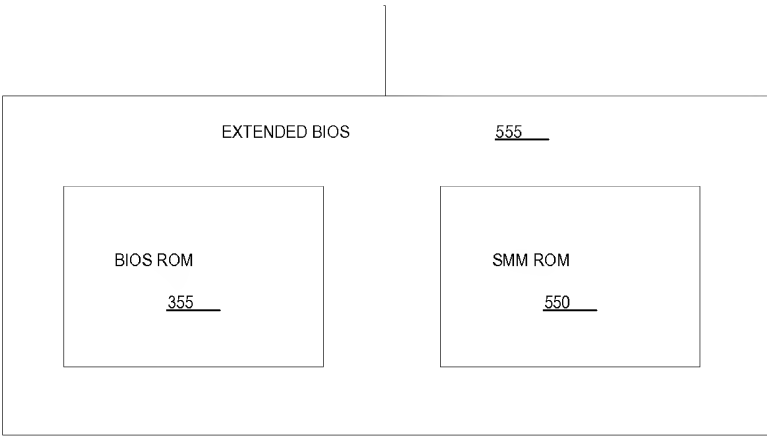
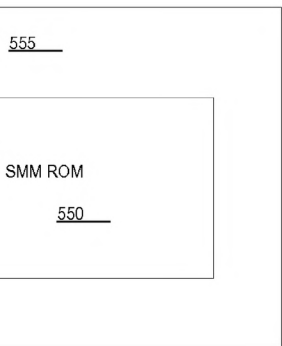


Fig. 7B



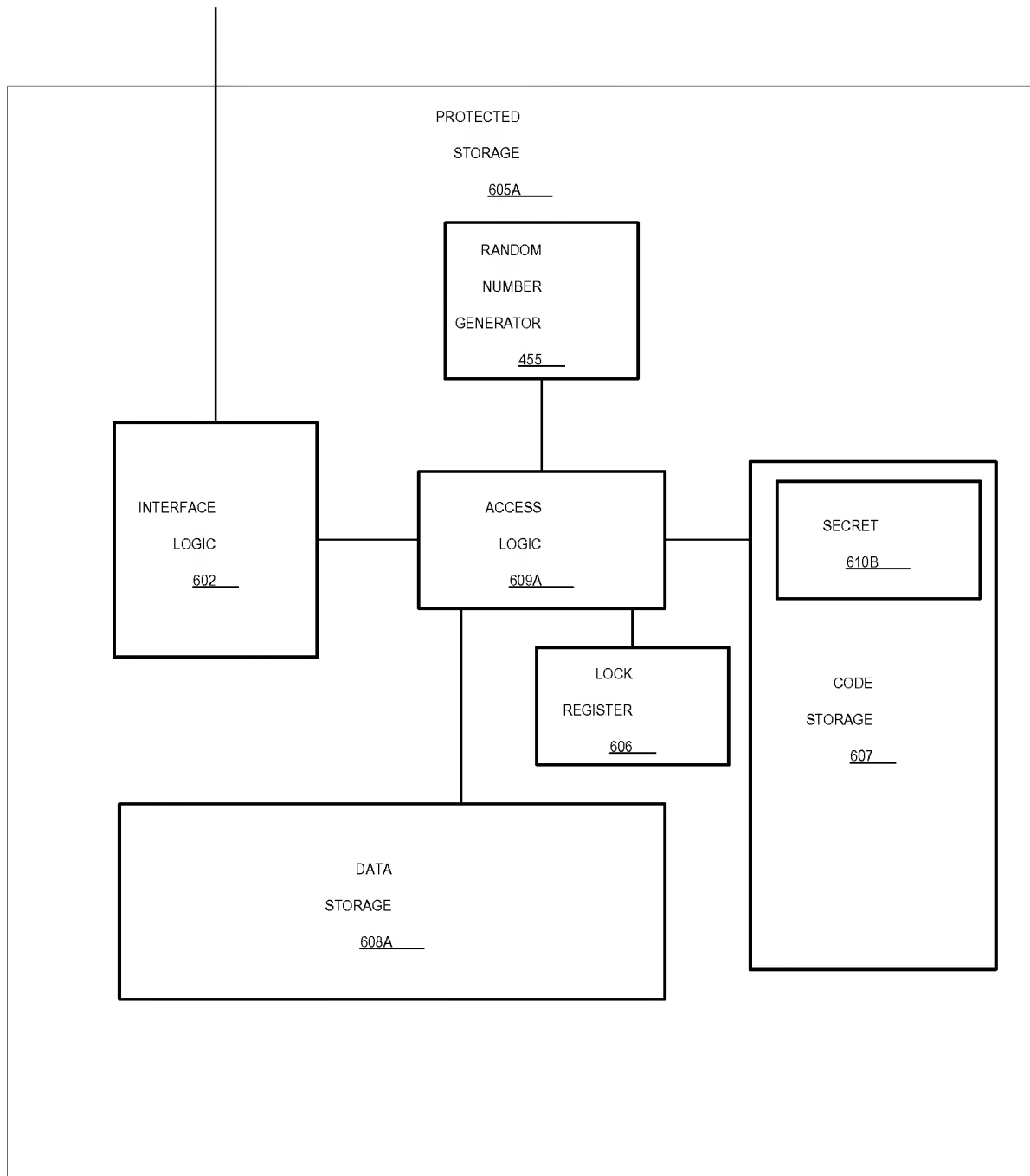


Fig. 7C

SECRET

610B

CODE

STORAGE

607

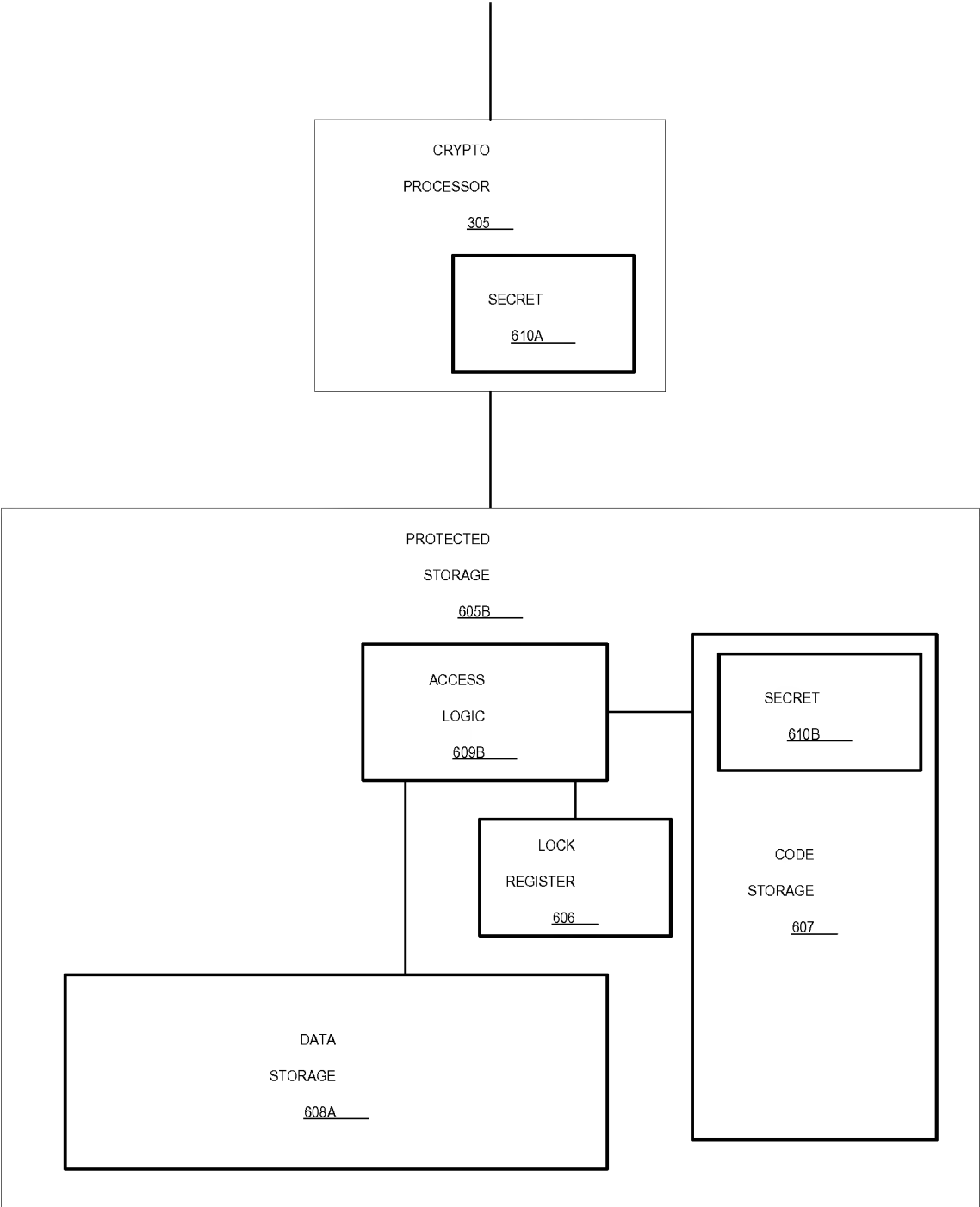


Fig. 7D

SECRET

610B

CODE

TORAGE

607

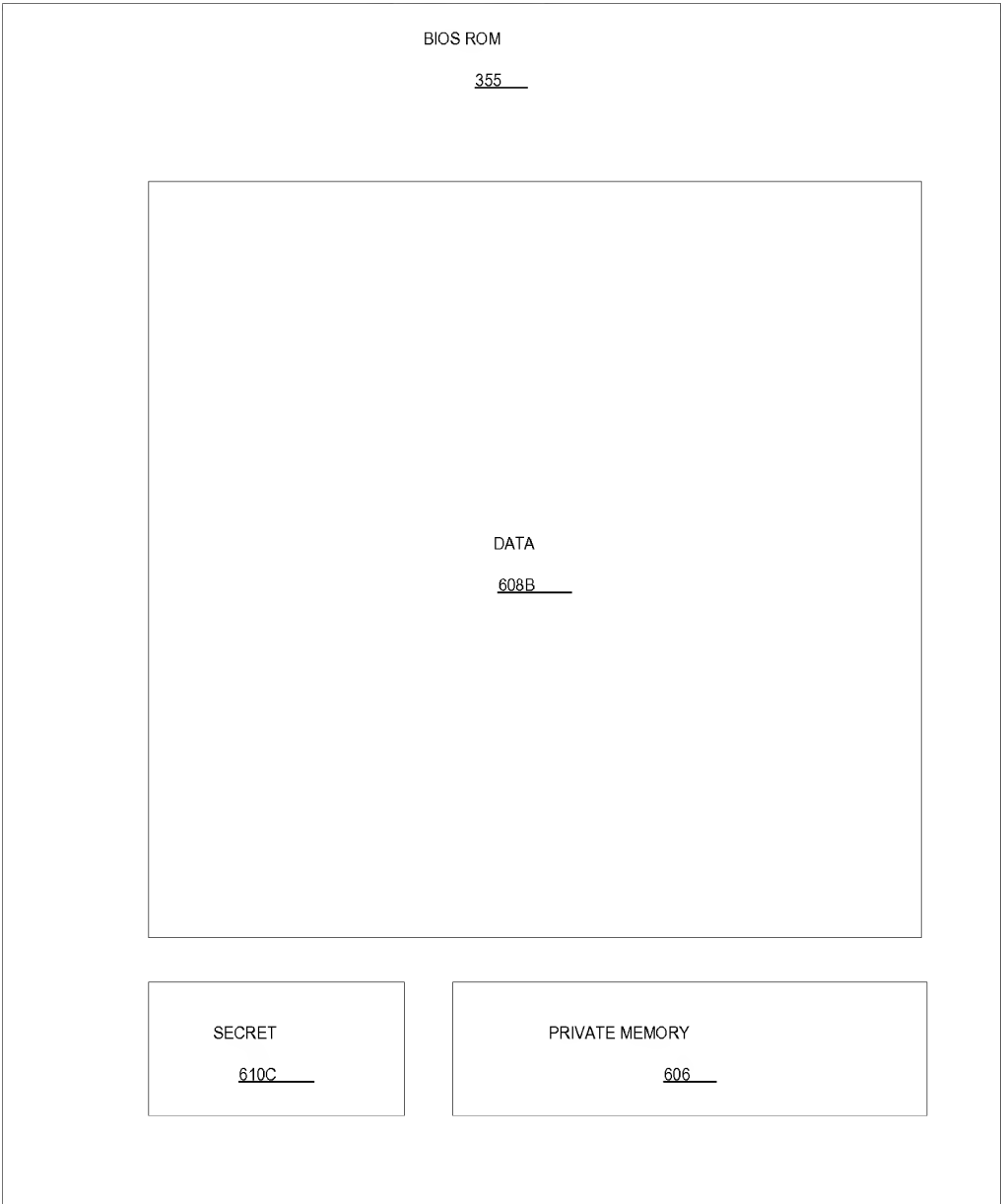
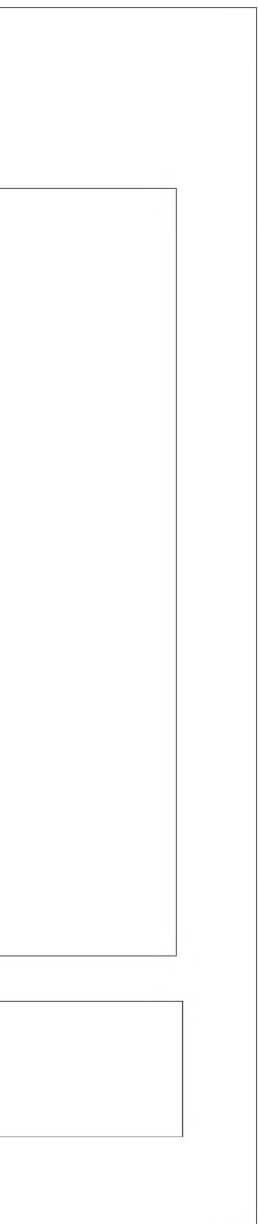


Fig. 8A



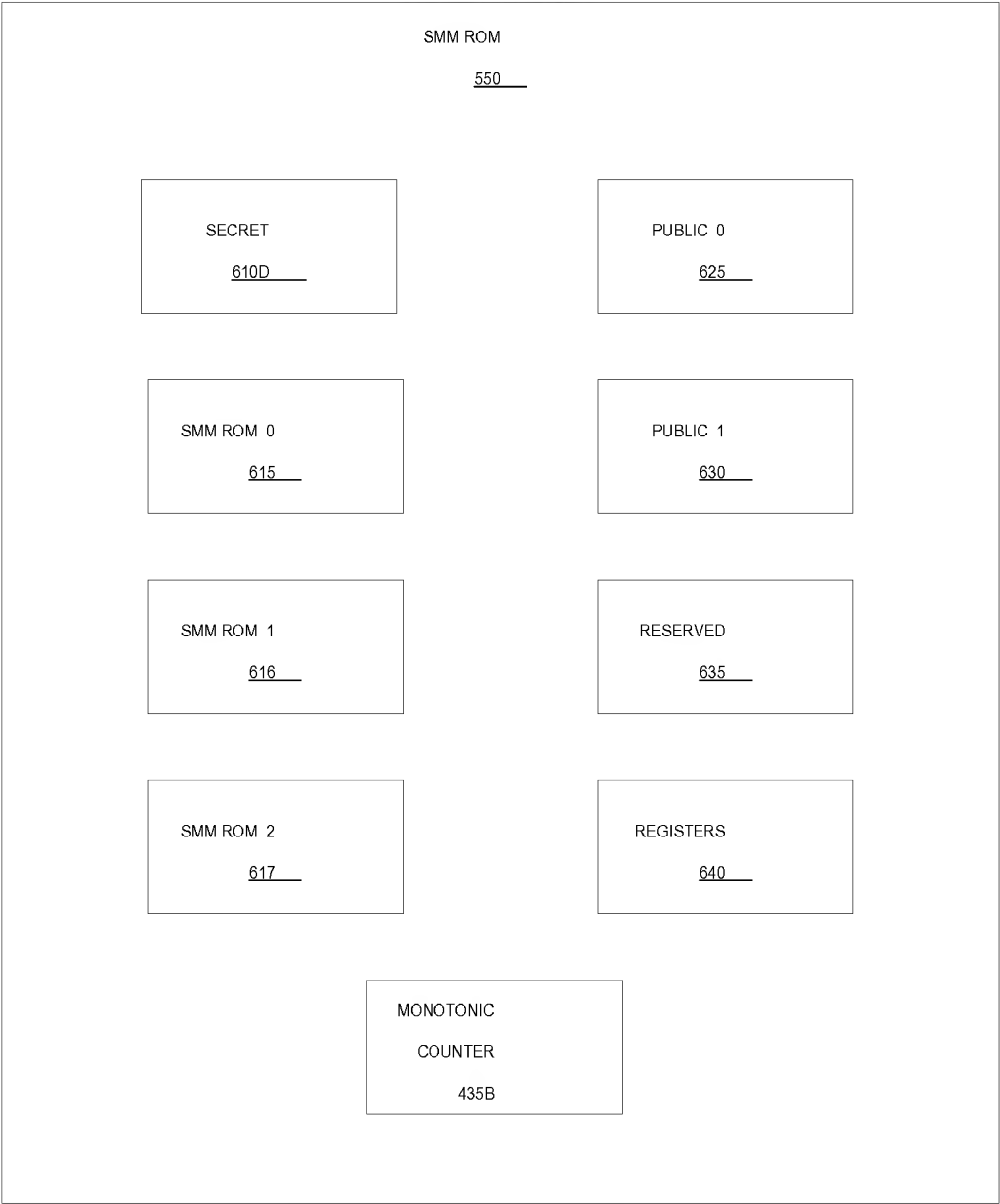


Fig. 8B

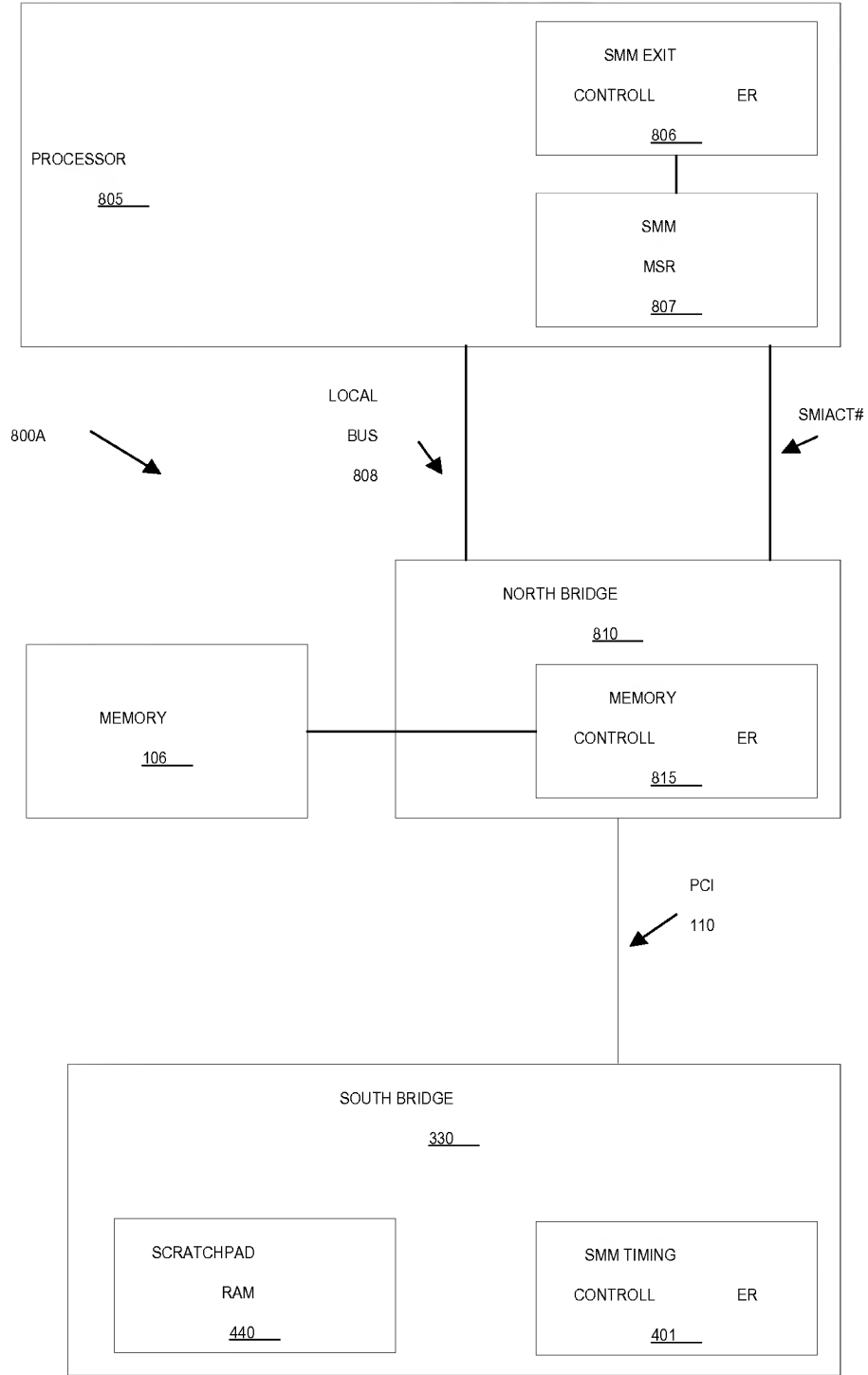


Fig. 9A

MIACT#

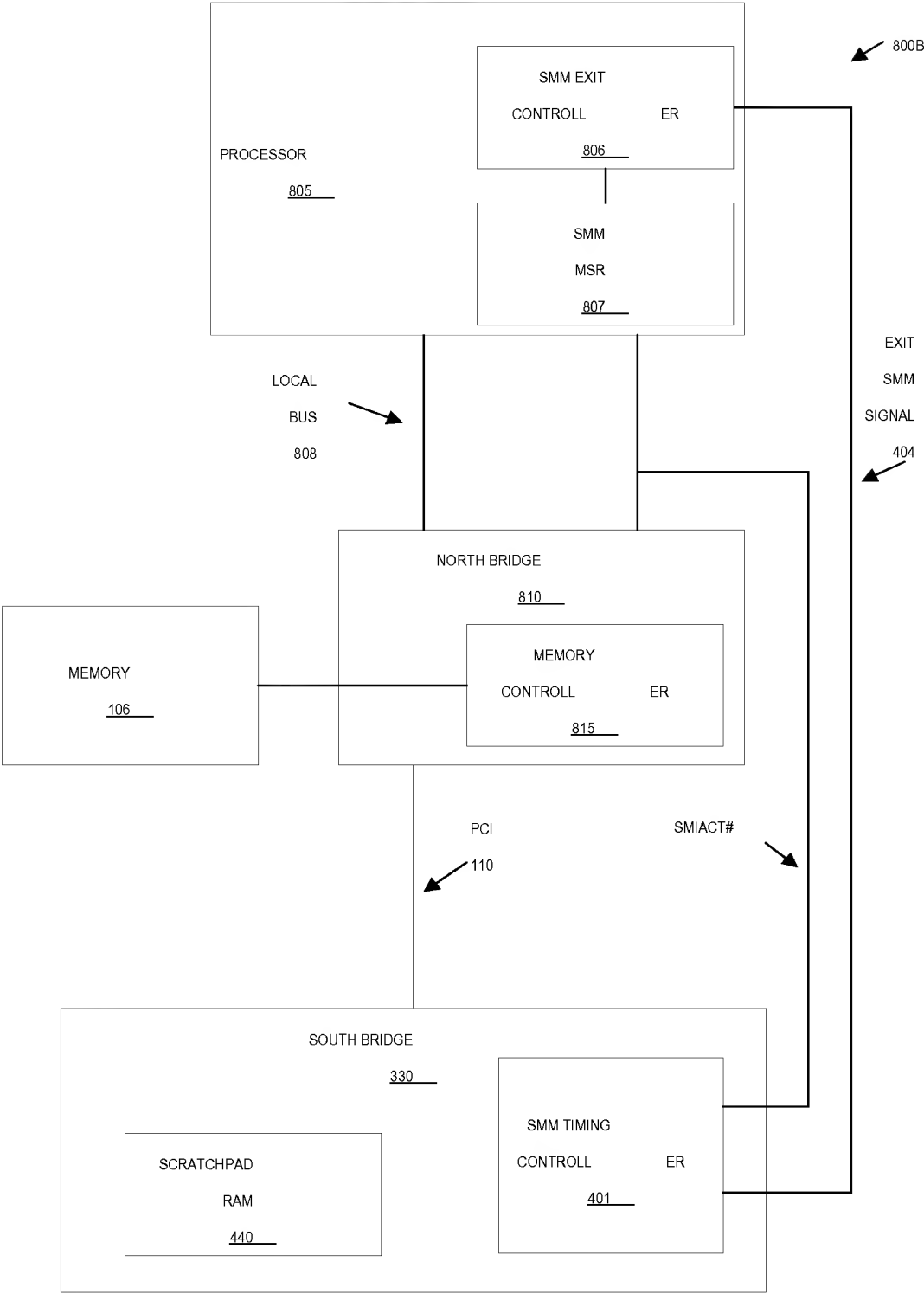
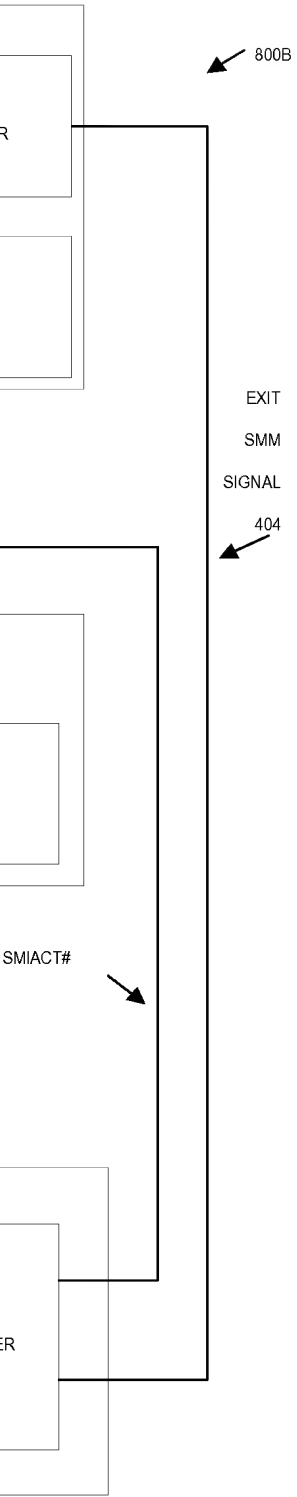


Fig. 9B



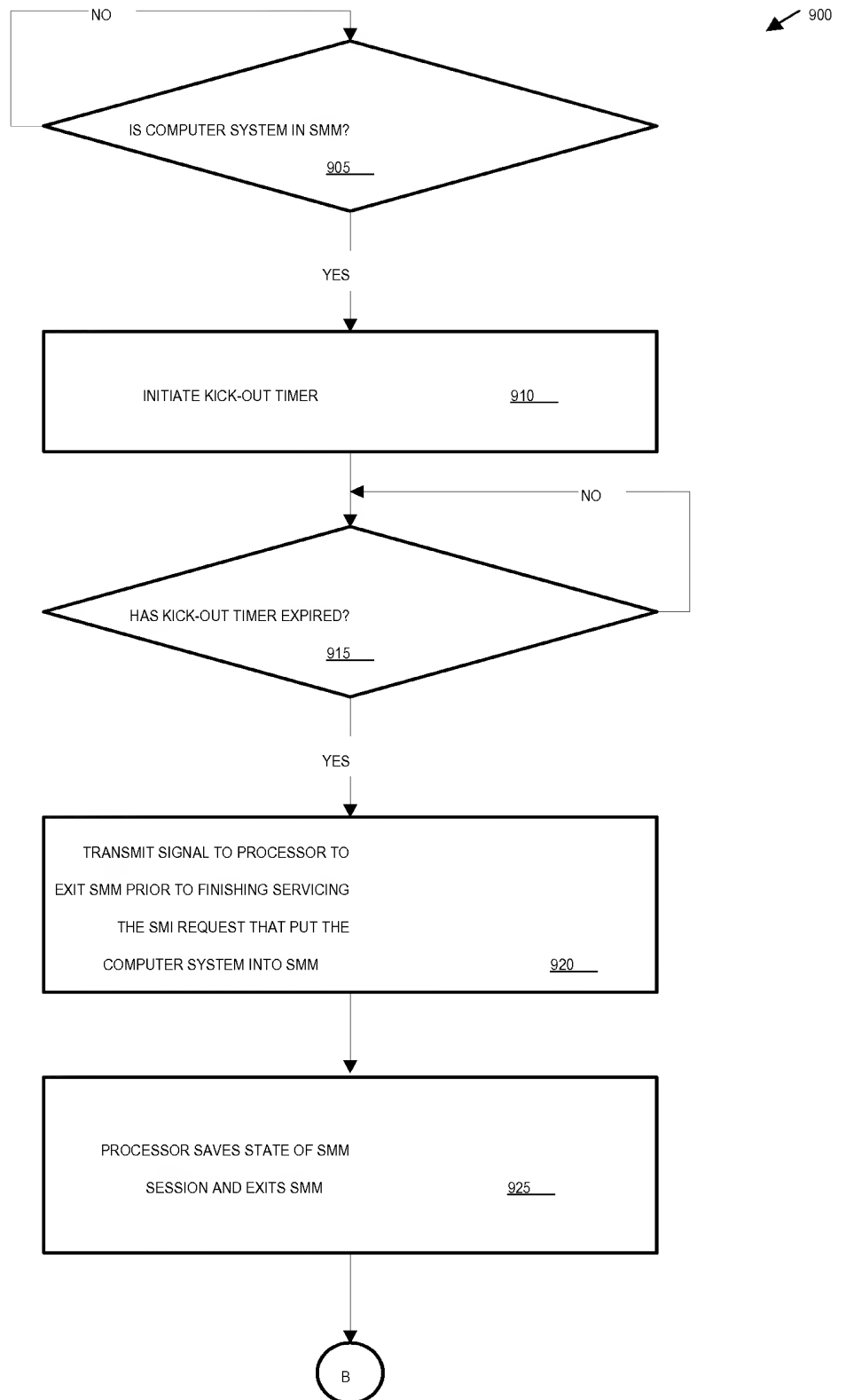
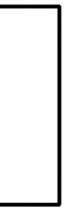
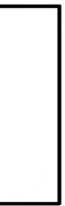
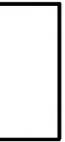


Fig. 10A

900



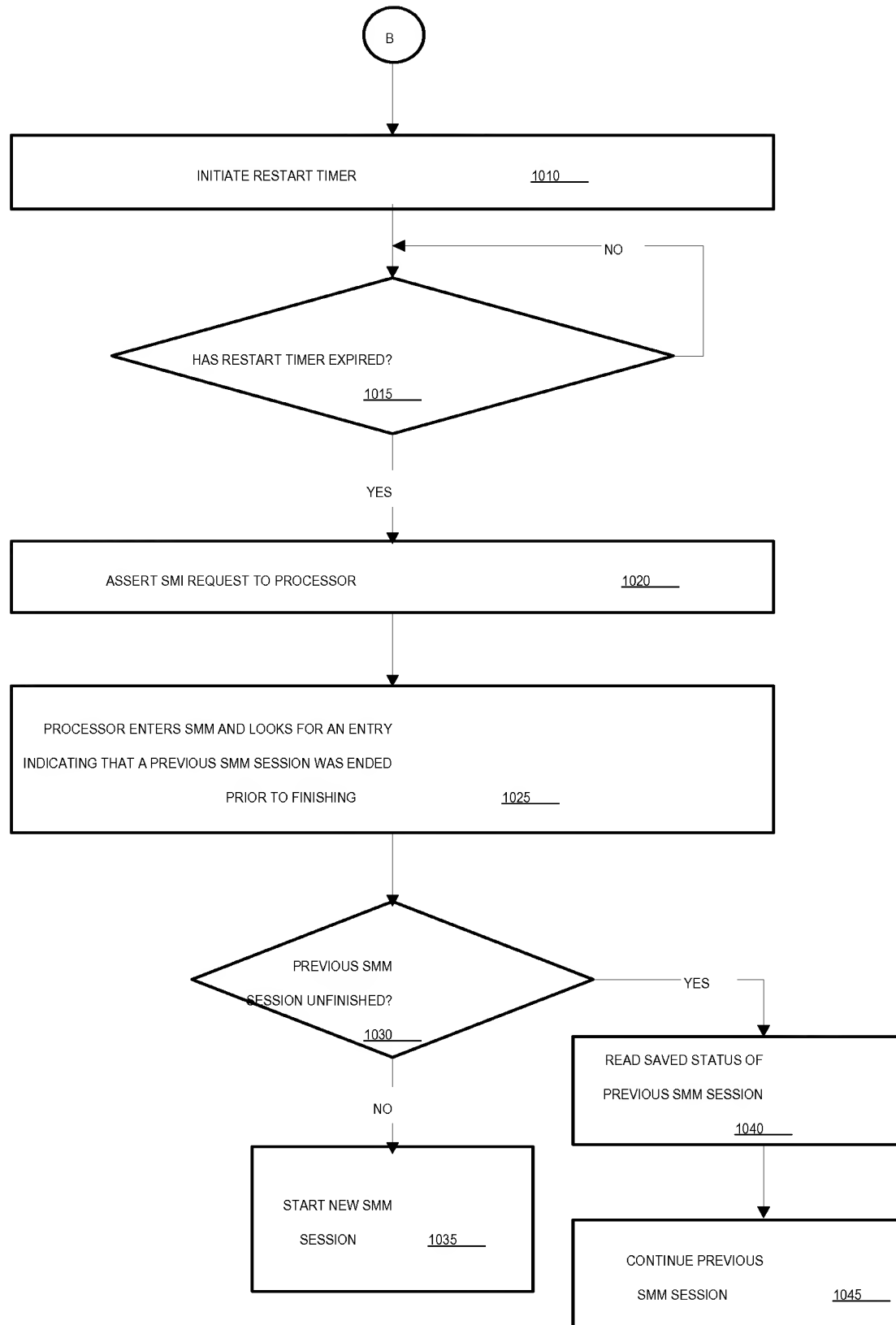
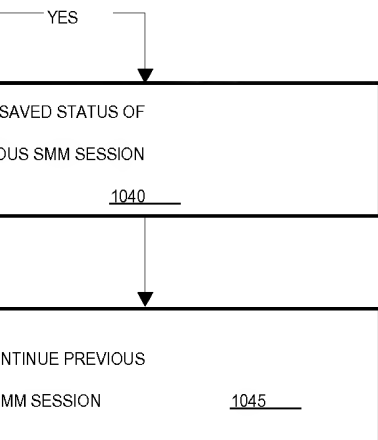


Fig. 10B



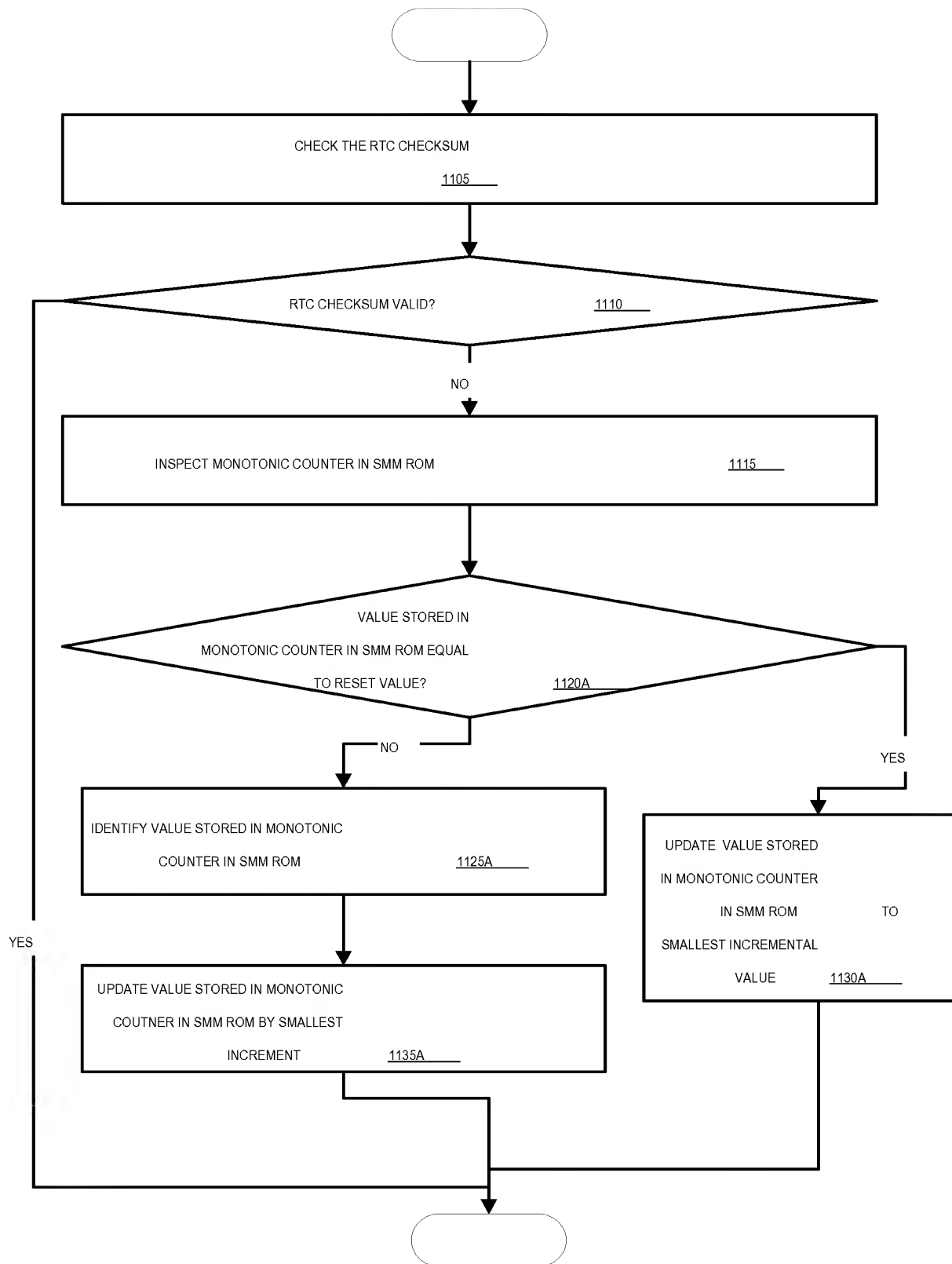
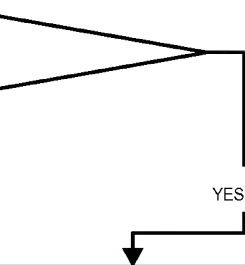
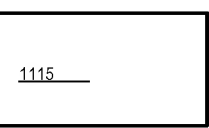
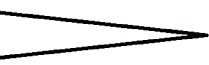


Fig. 11A

1100A



YES

VALUE STORED
TONIC COUNTER
IN SMM ROM TO
ST INCREMENTAL
VALUE 1130A



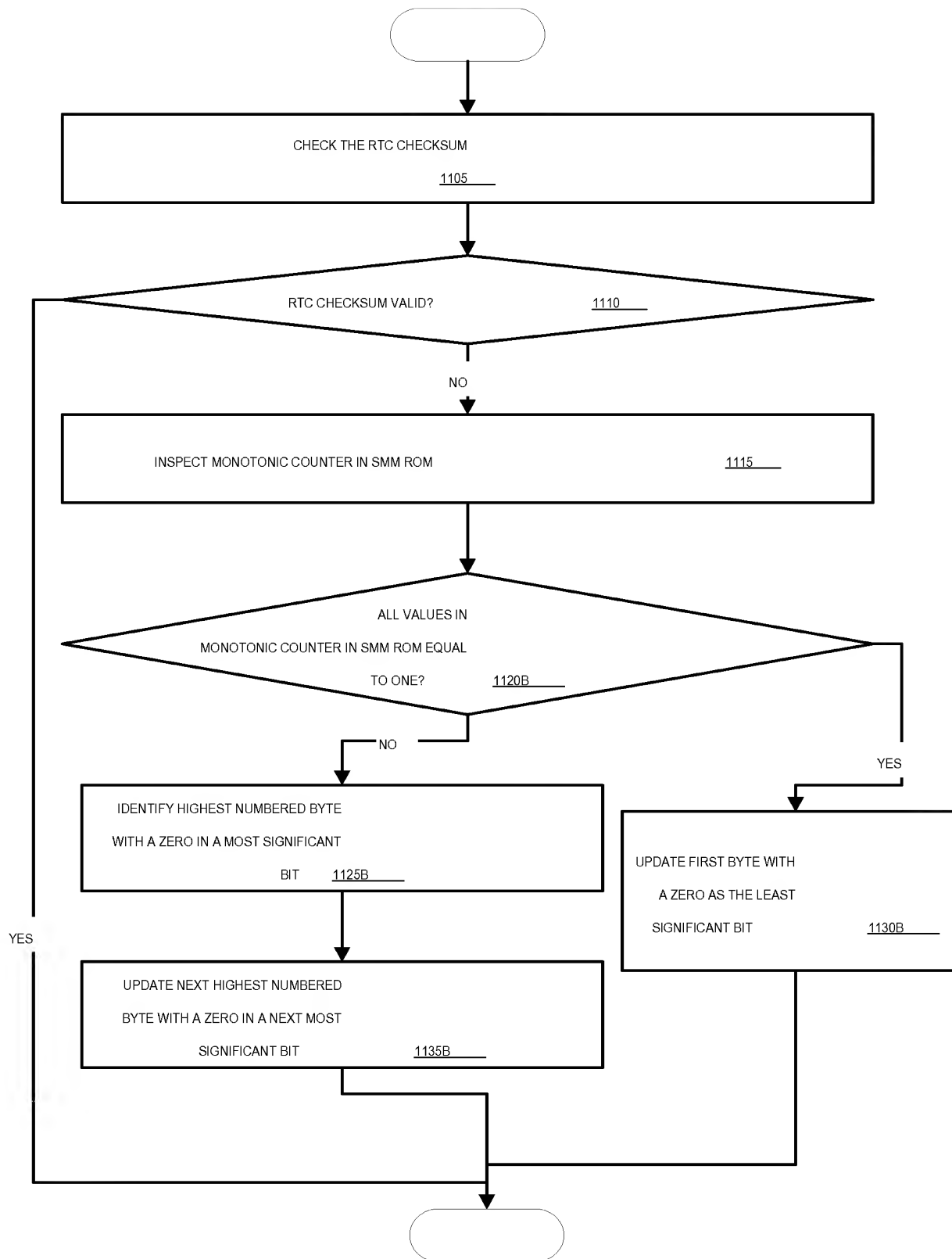
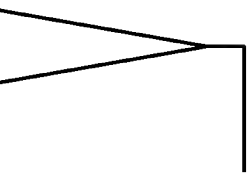
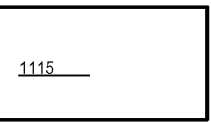
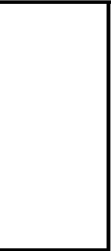
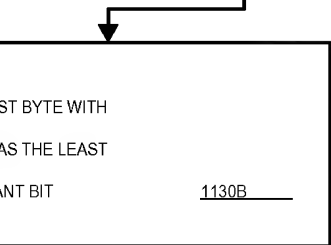


Fig. 11B

1100B



YES



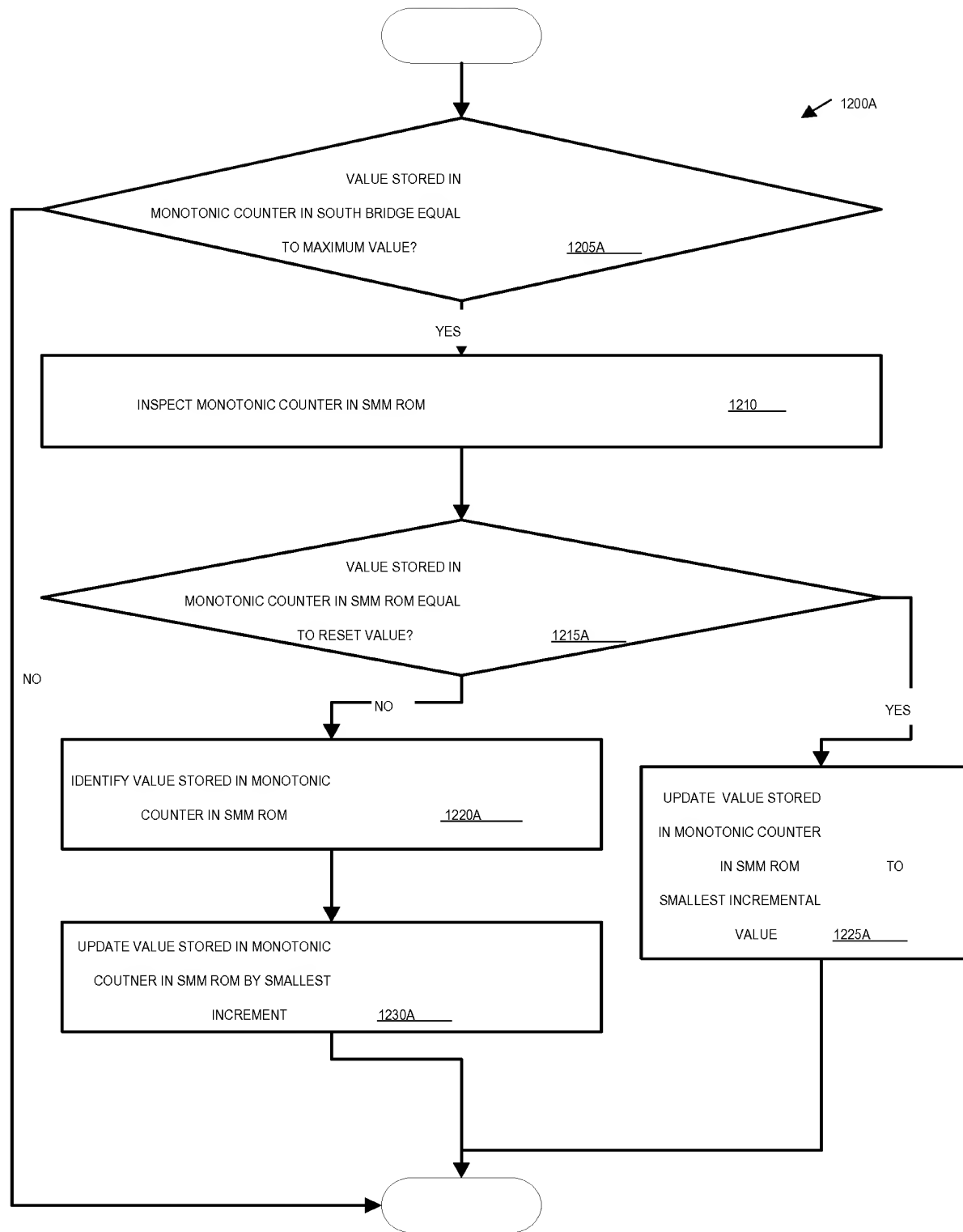
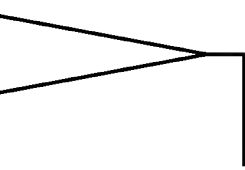
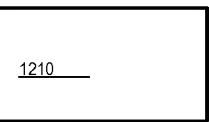
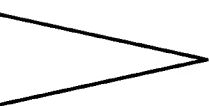
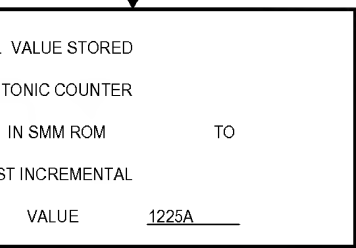


Fig. 12A

1200A



YES



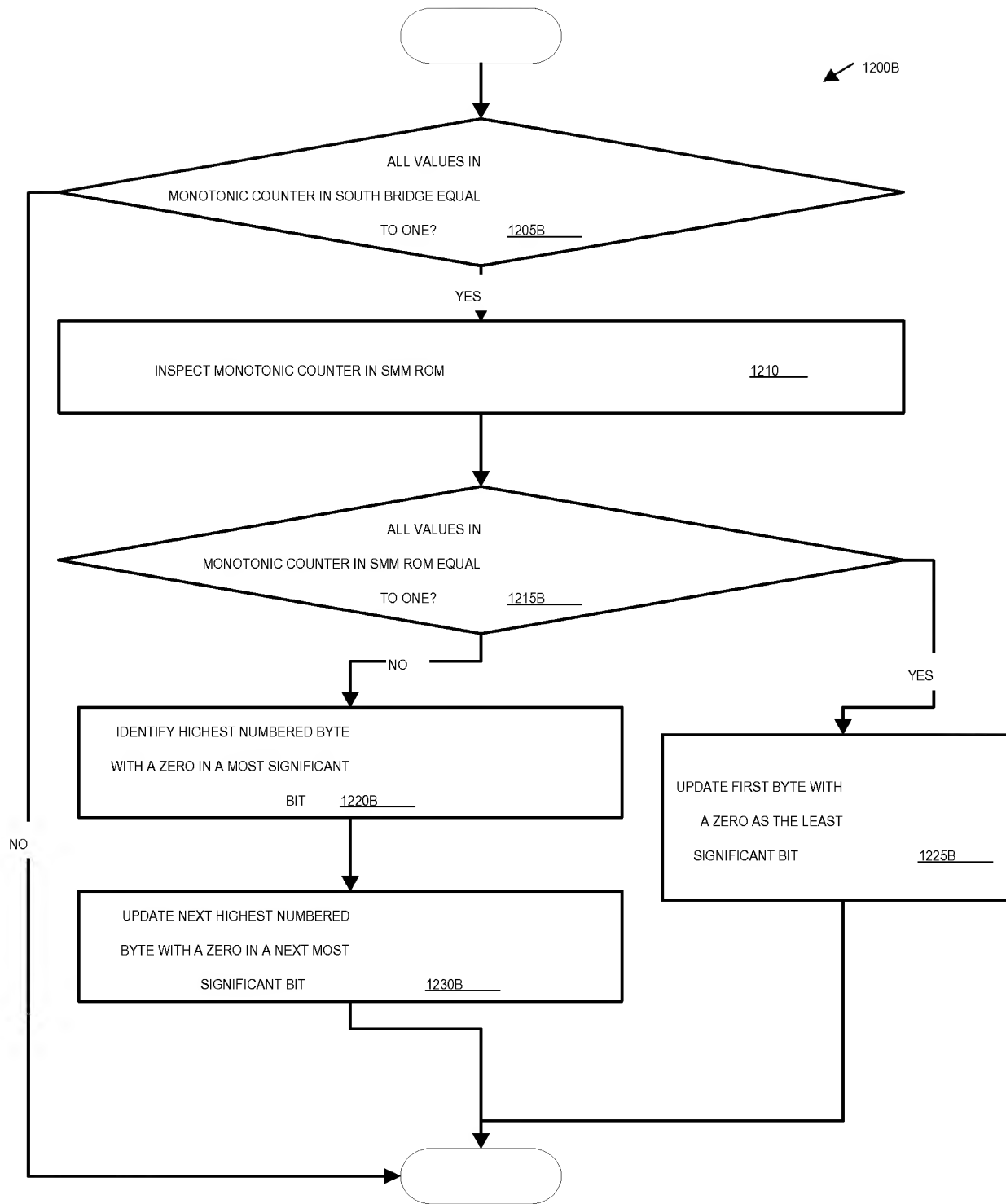
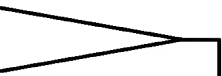
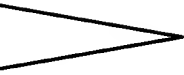
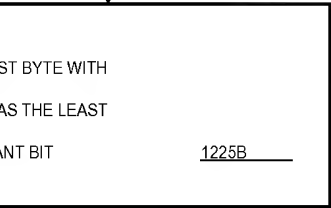


Fig. 12B

1200B



YES



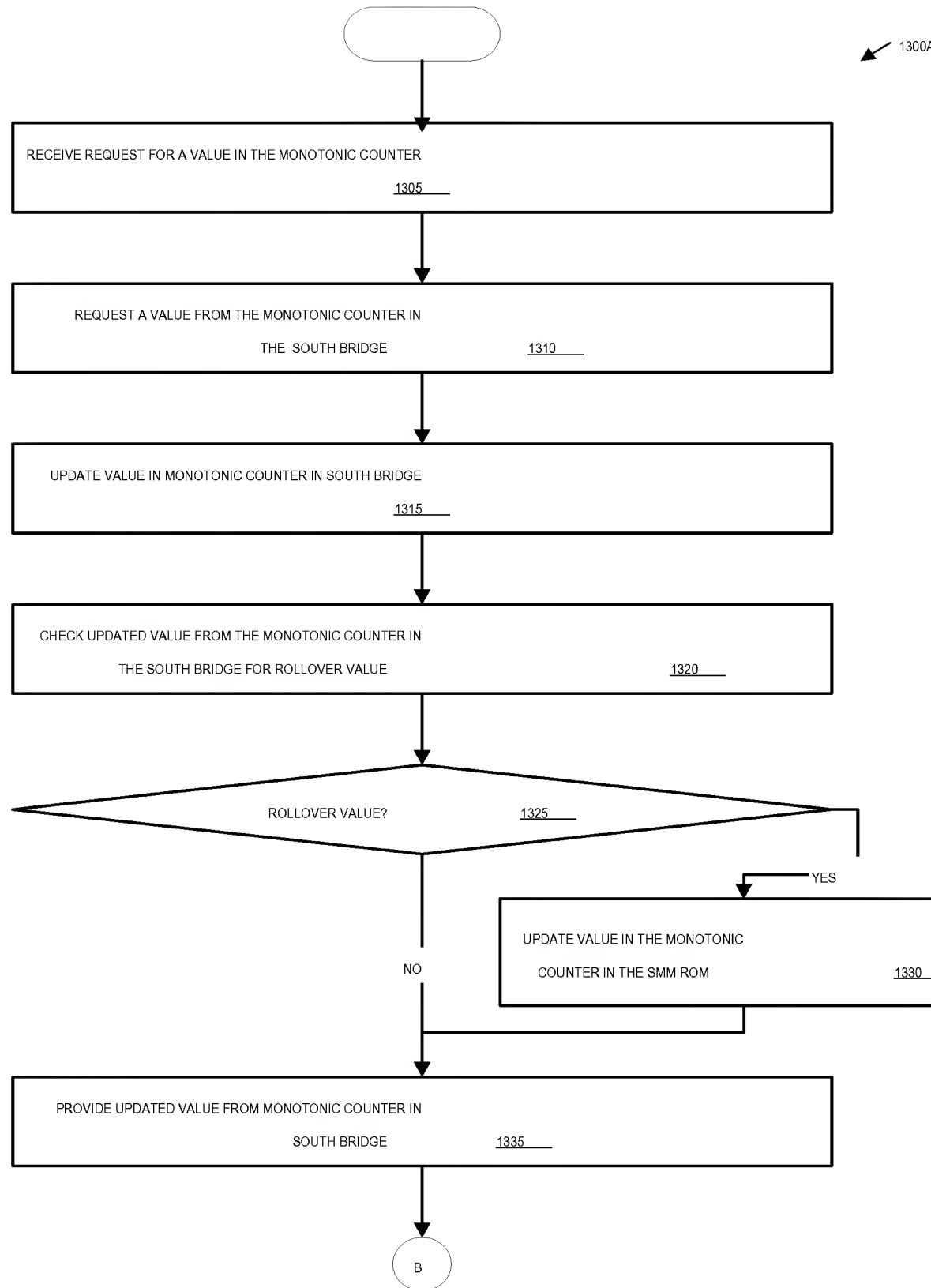
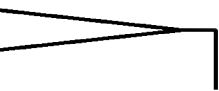


Fig. 13A

1300A

20



YES

NOTONIC

OM

1330

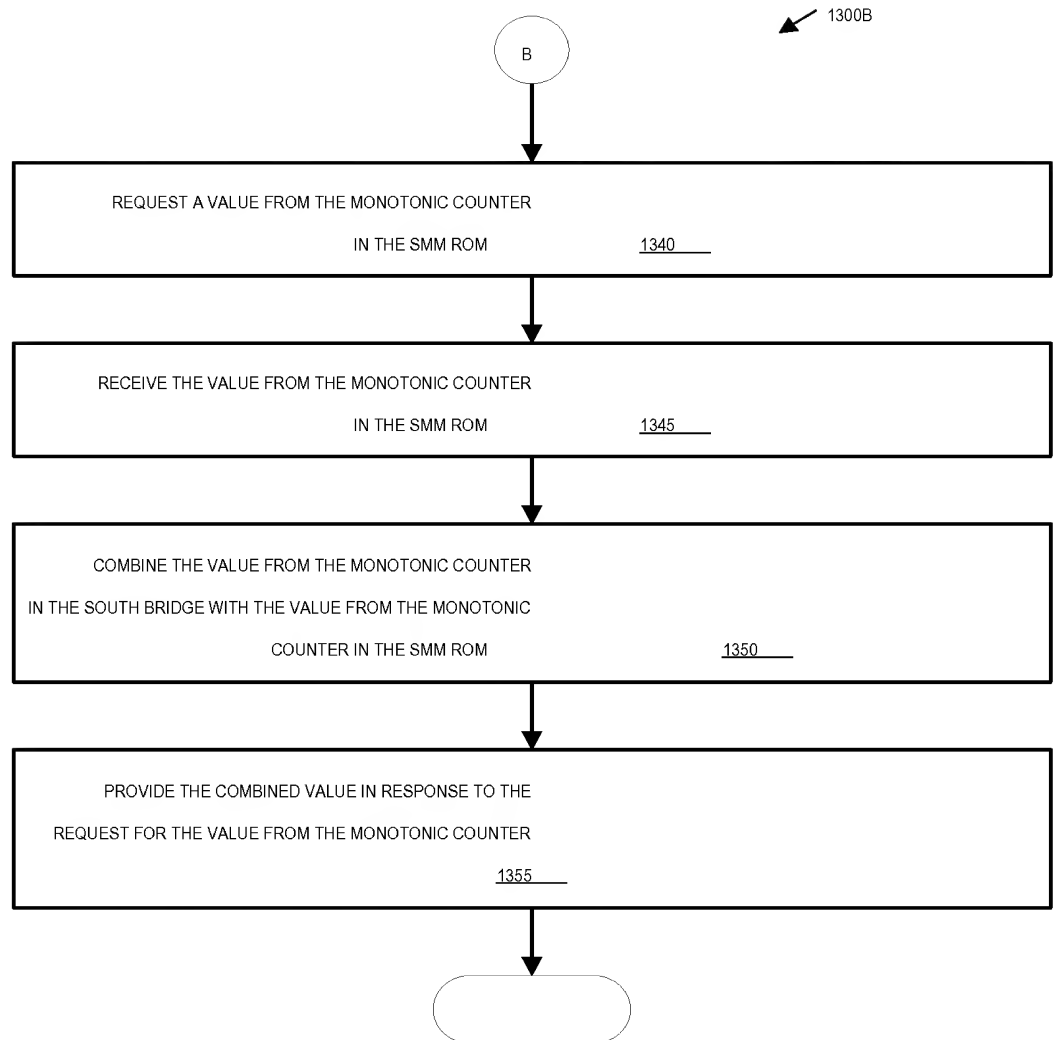


Fig. 13B

1300B

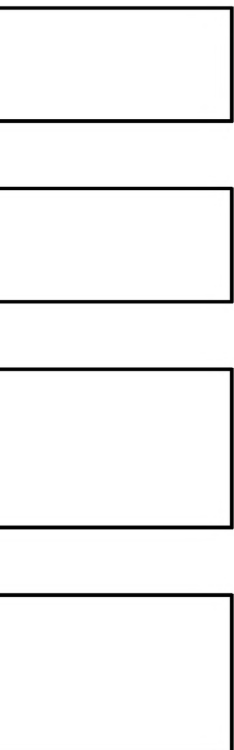


Fig. 13B

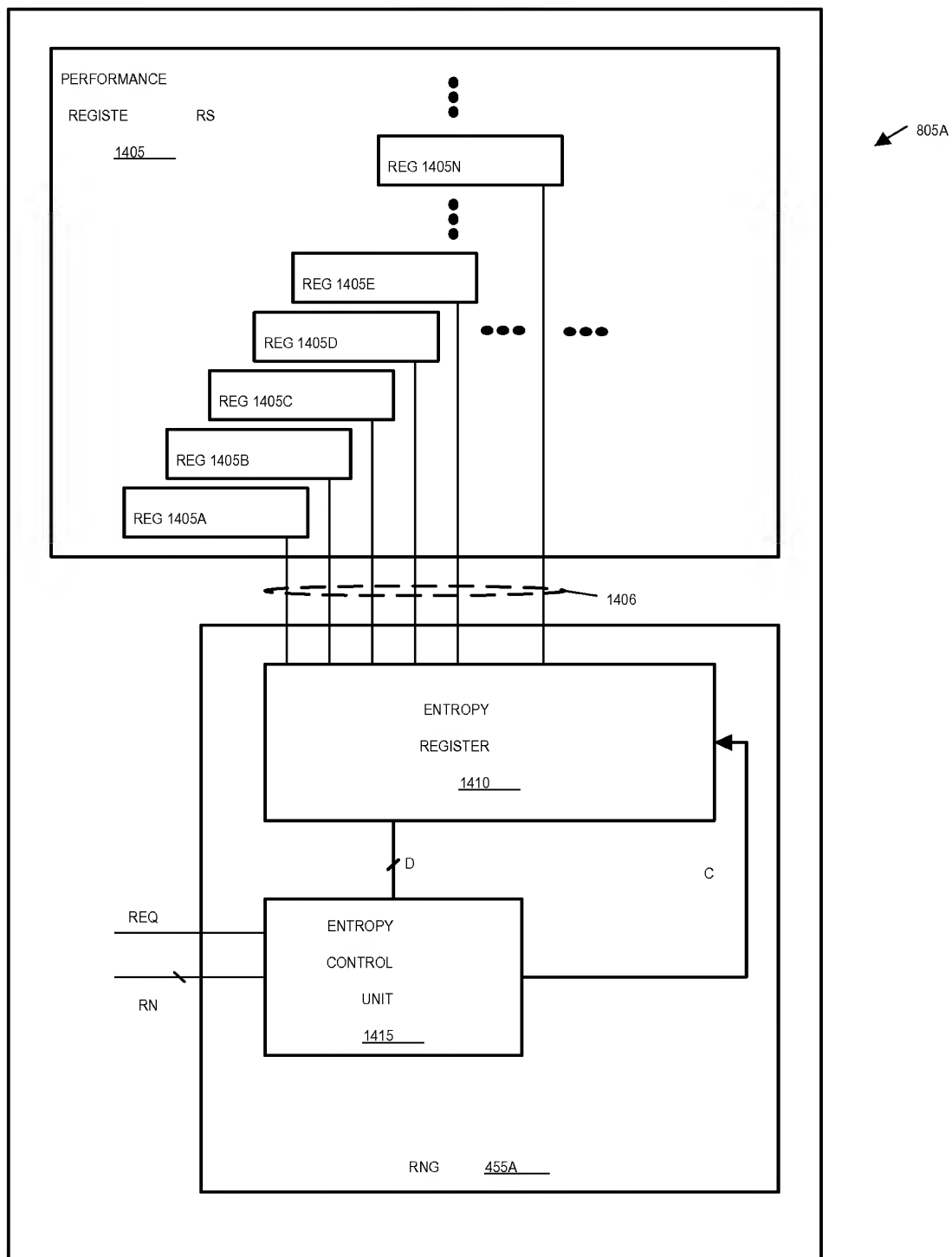


Fig. 14A



805A

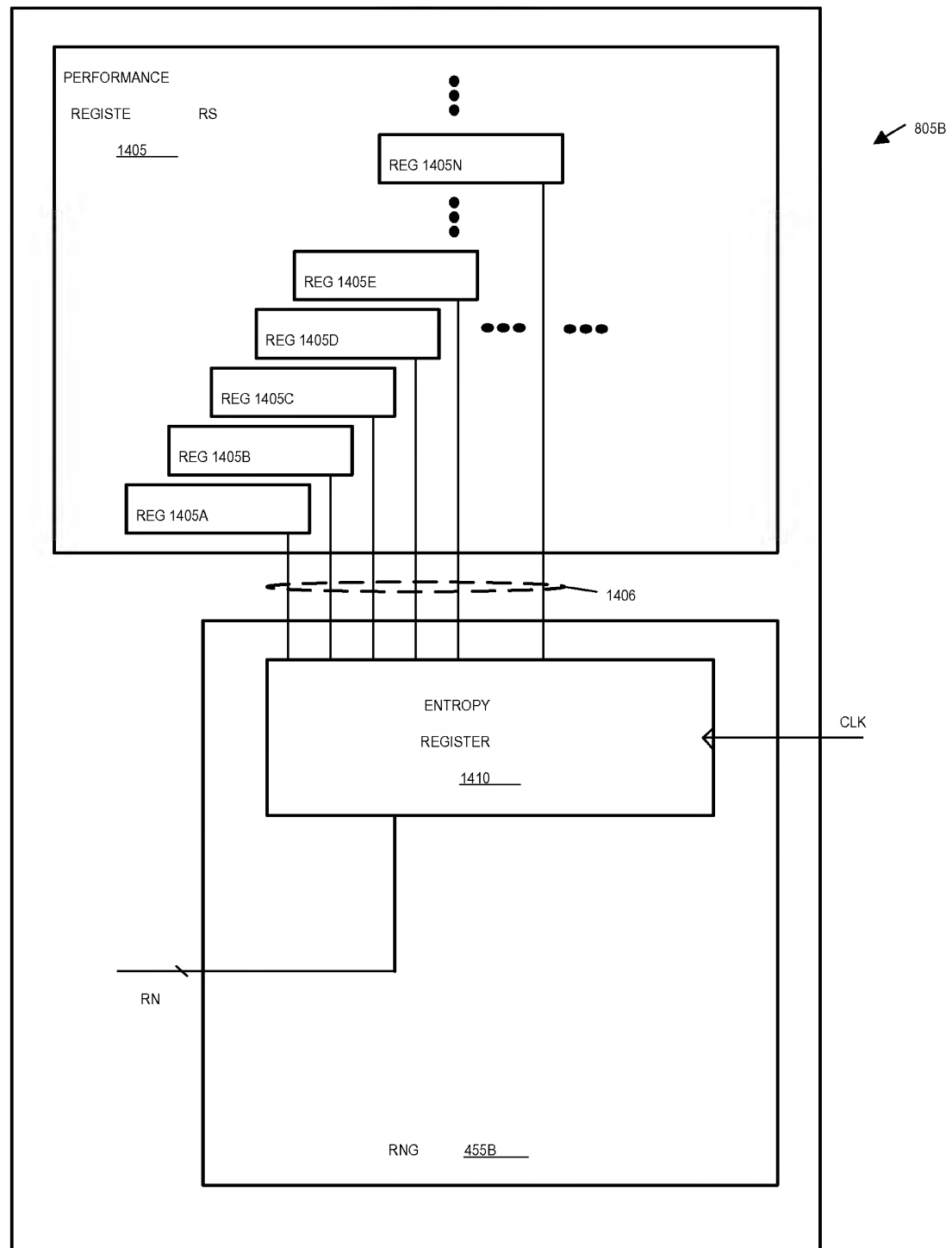


Fig. 14B



805B

CLK

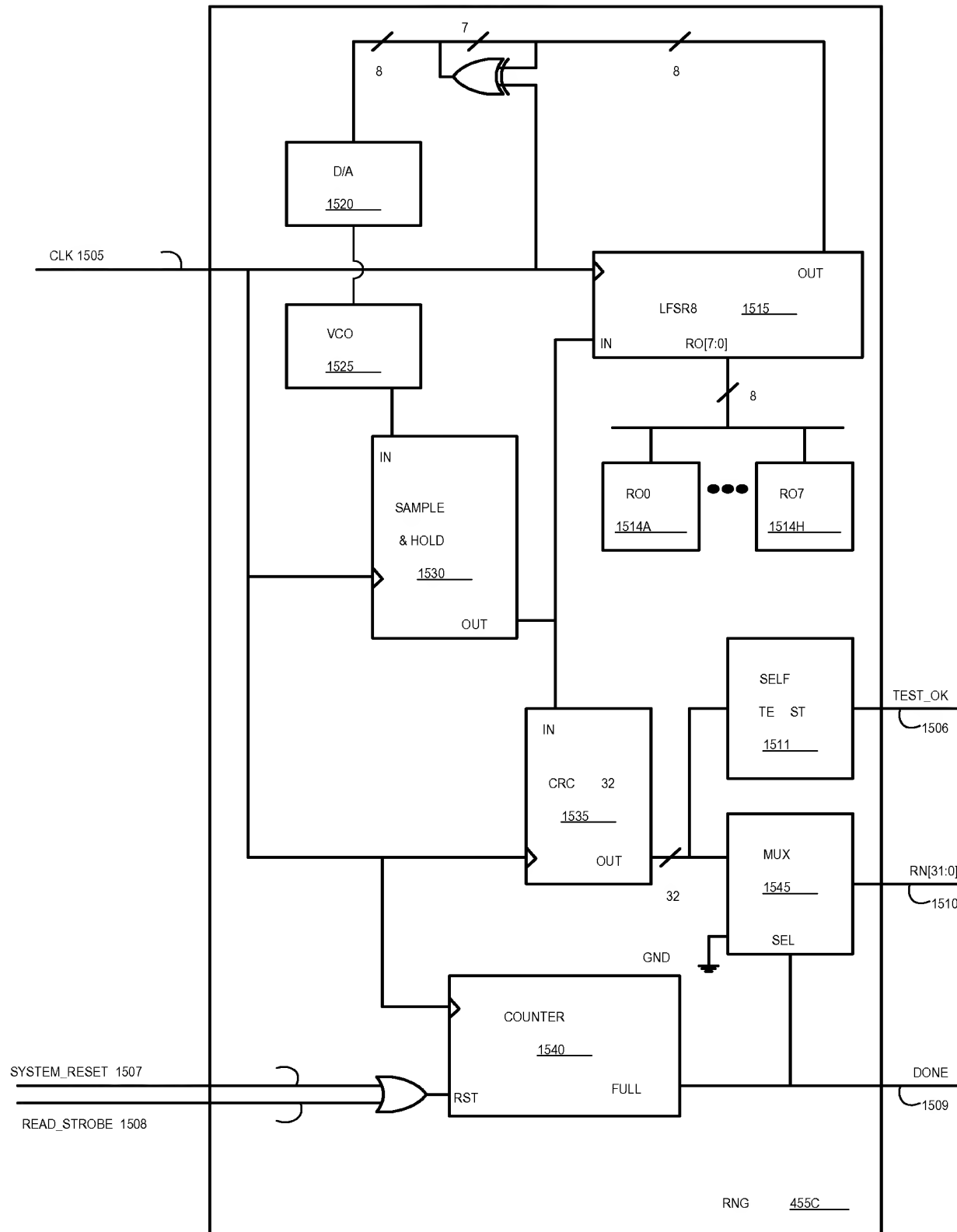
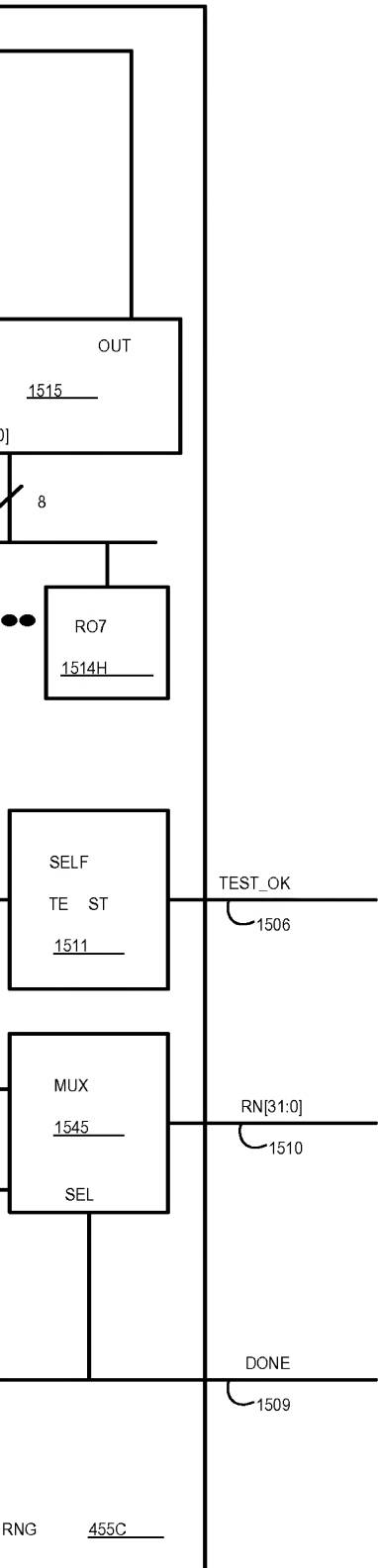


Fig. 15



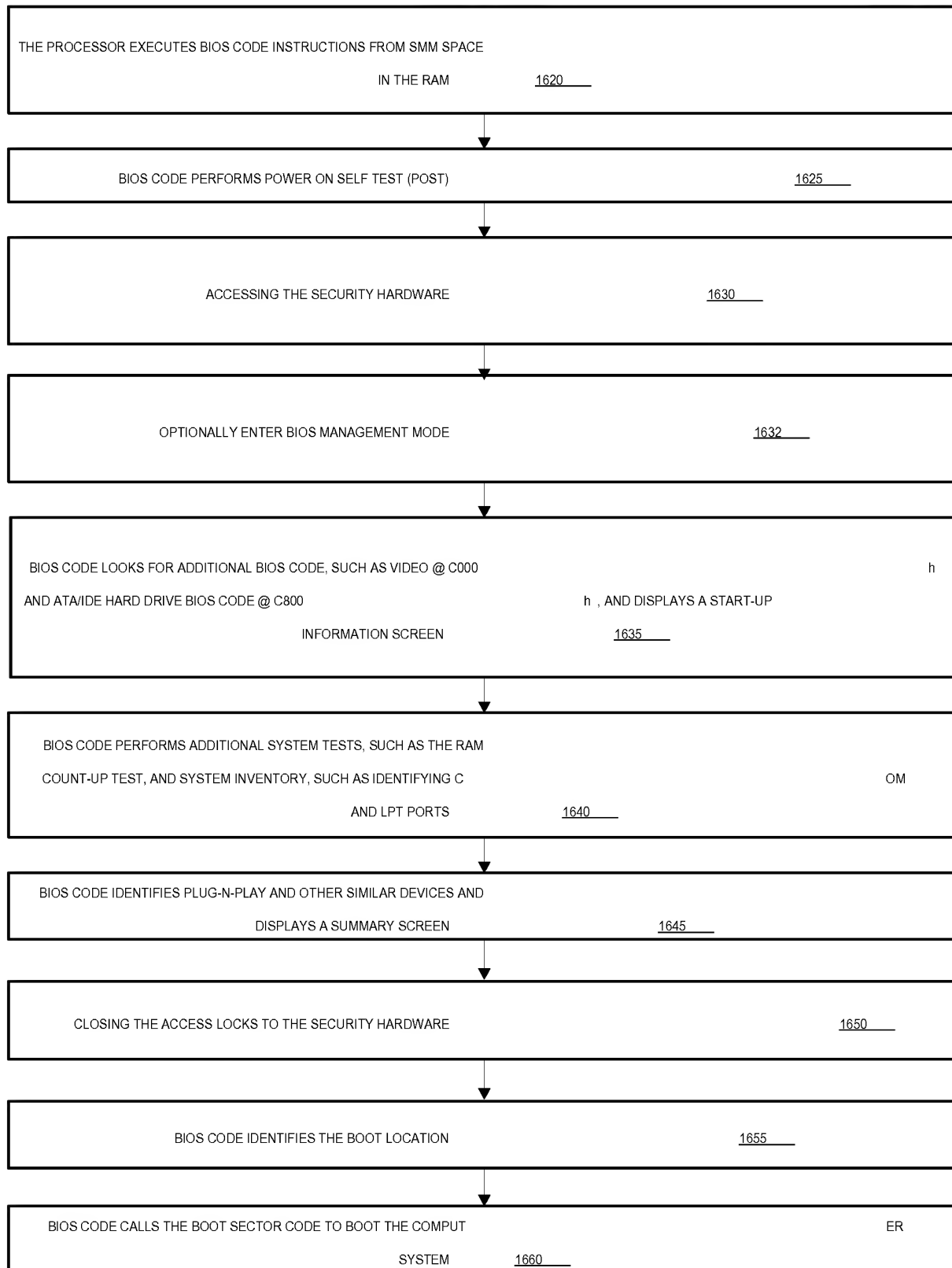


Fig. 16A

1600A

1625

1630

1632

h

TART-UP

OM

1650

1655

ER

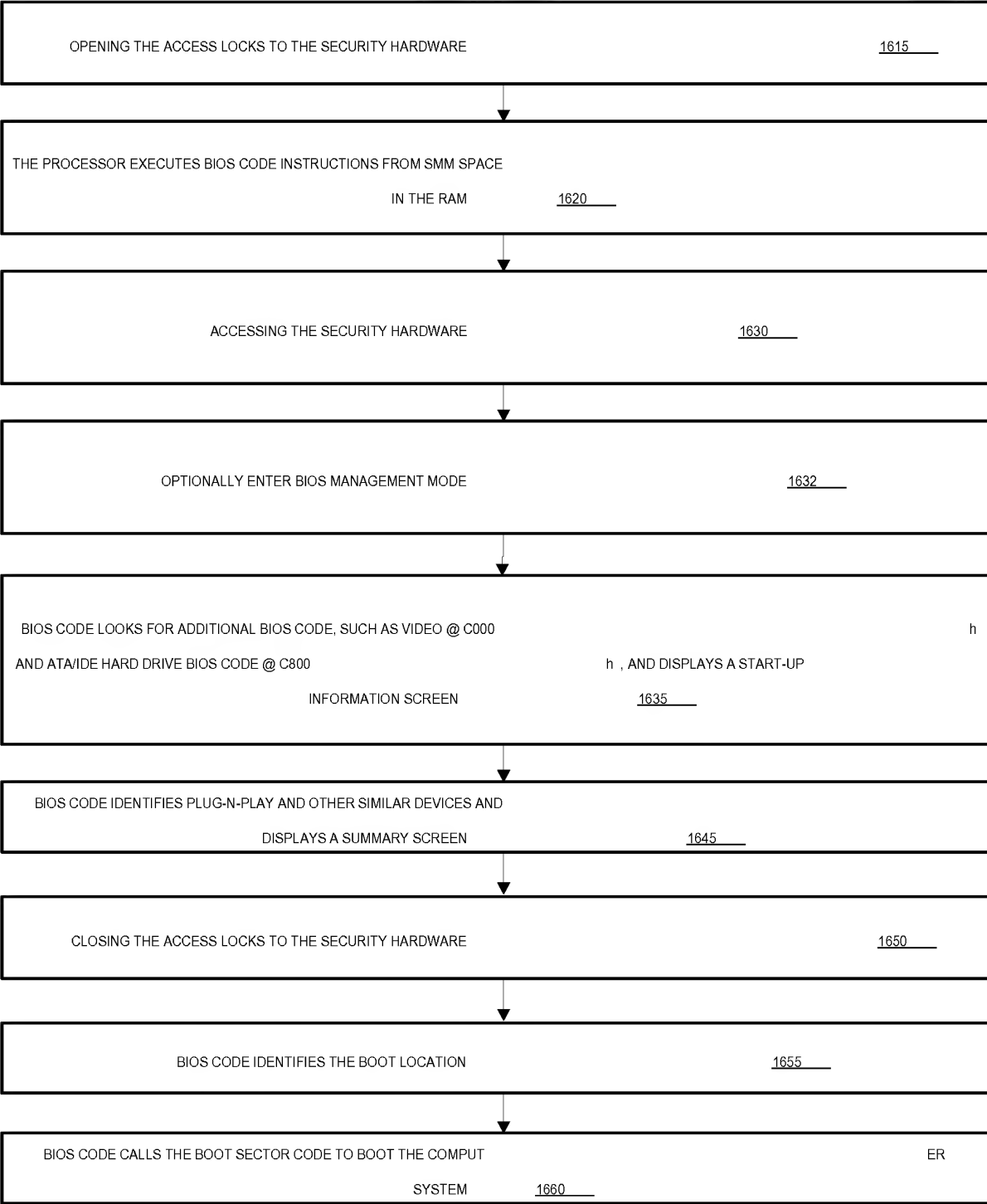


Fig. 16B

1600B

1615

1630

1632

h
A START-UP

1650

1655

ER

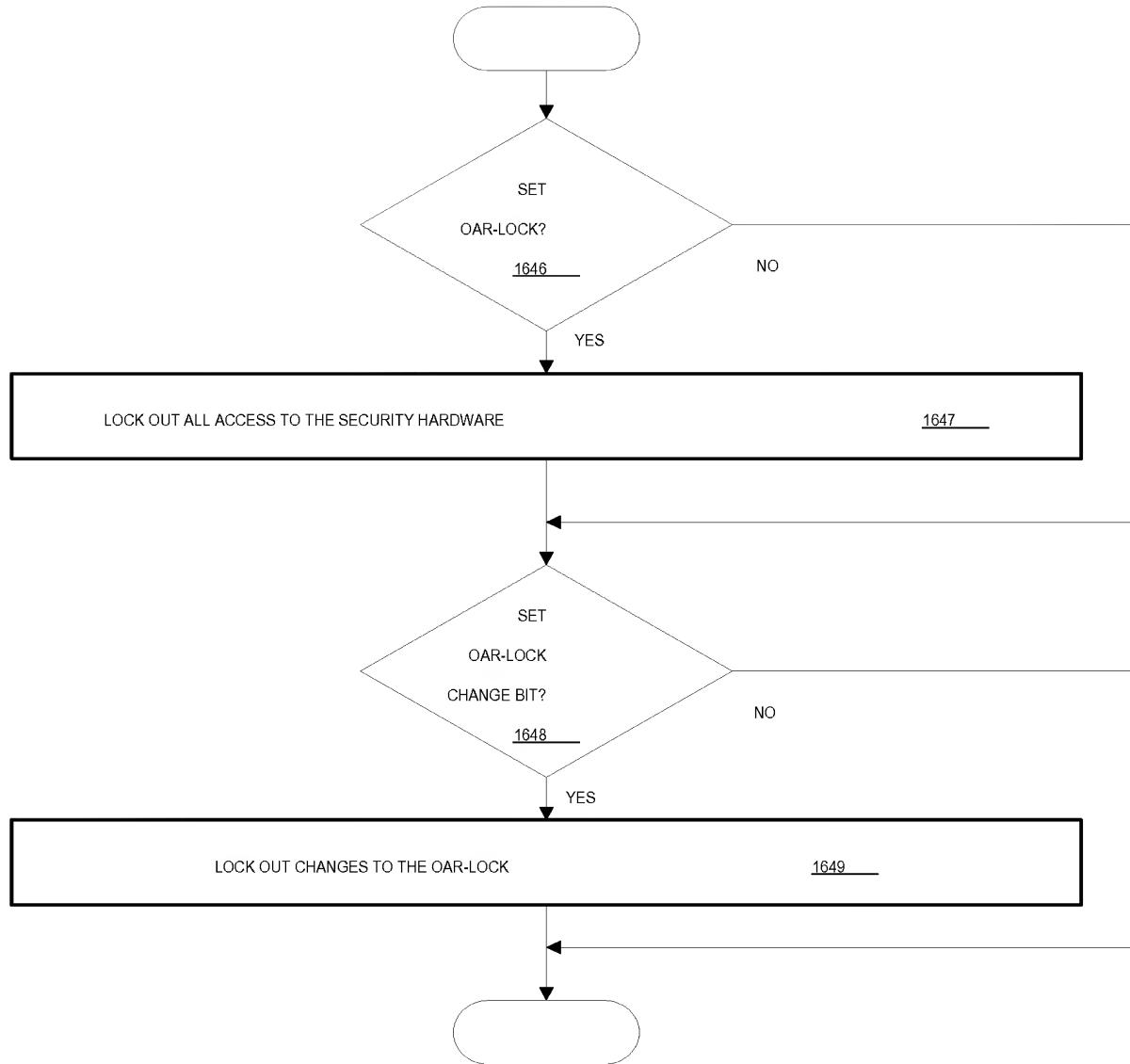


Fig. 16C

1600C

1647

9

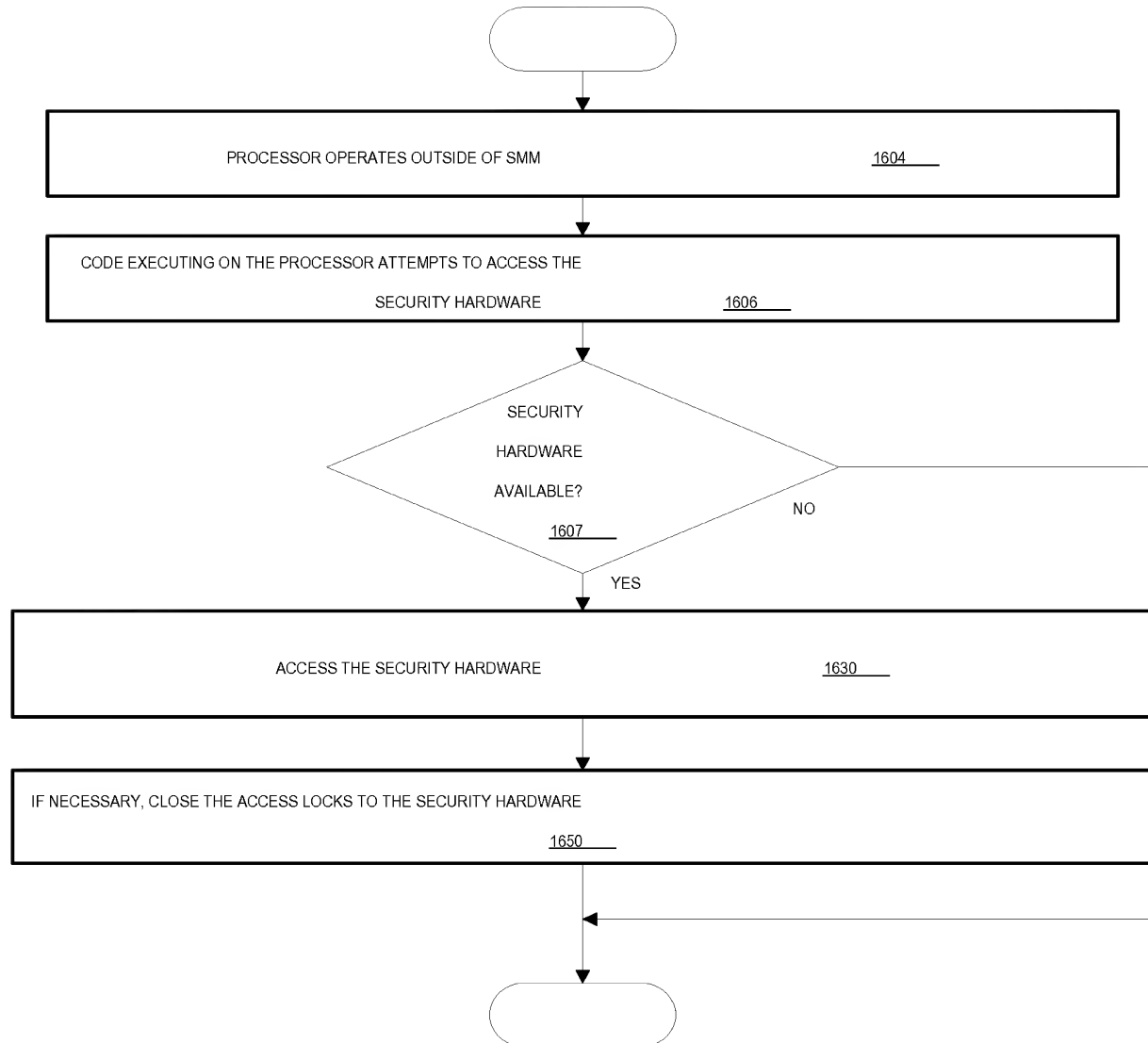


Fig. 16D

1600D

1604

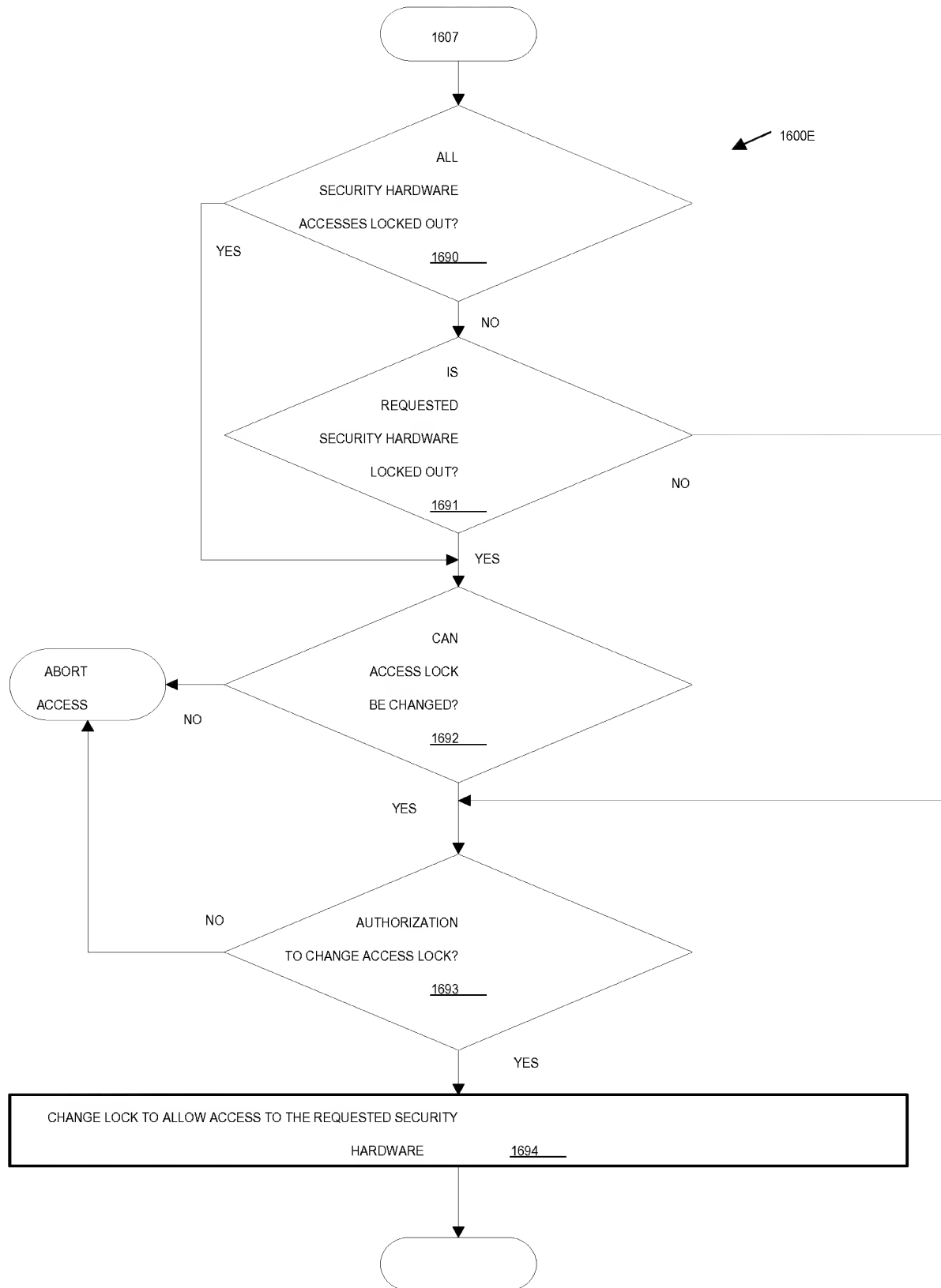
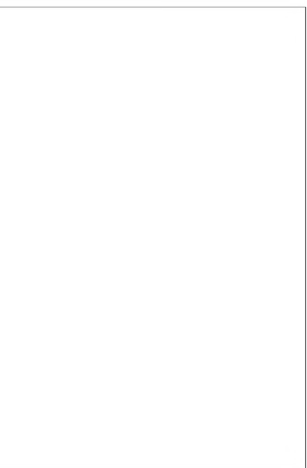


Fig. 16E

1600E



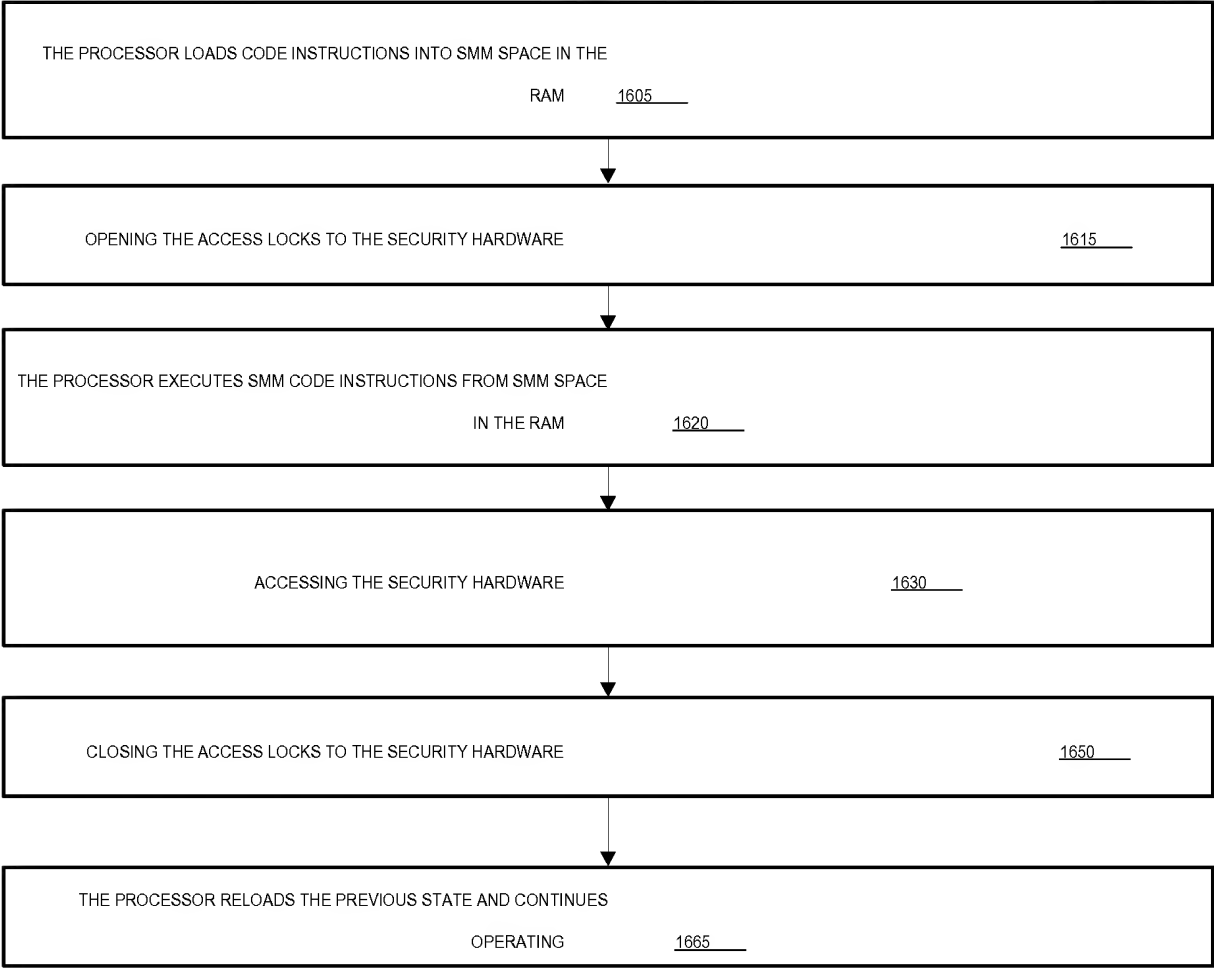


Fig. 16F

1600F

1615

1650

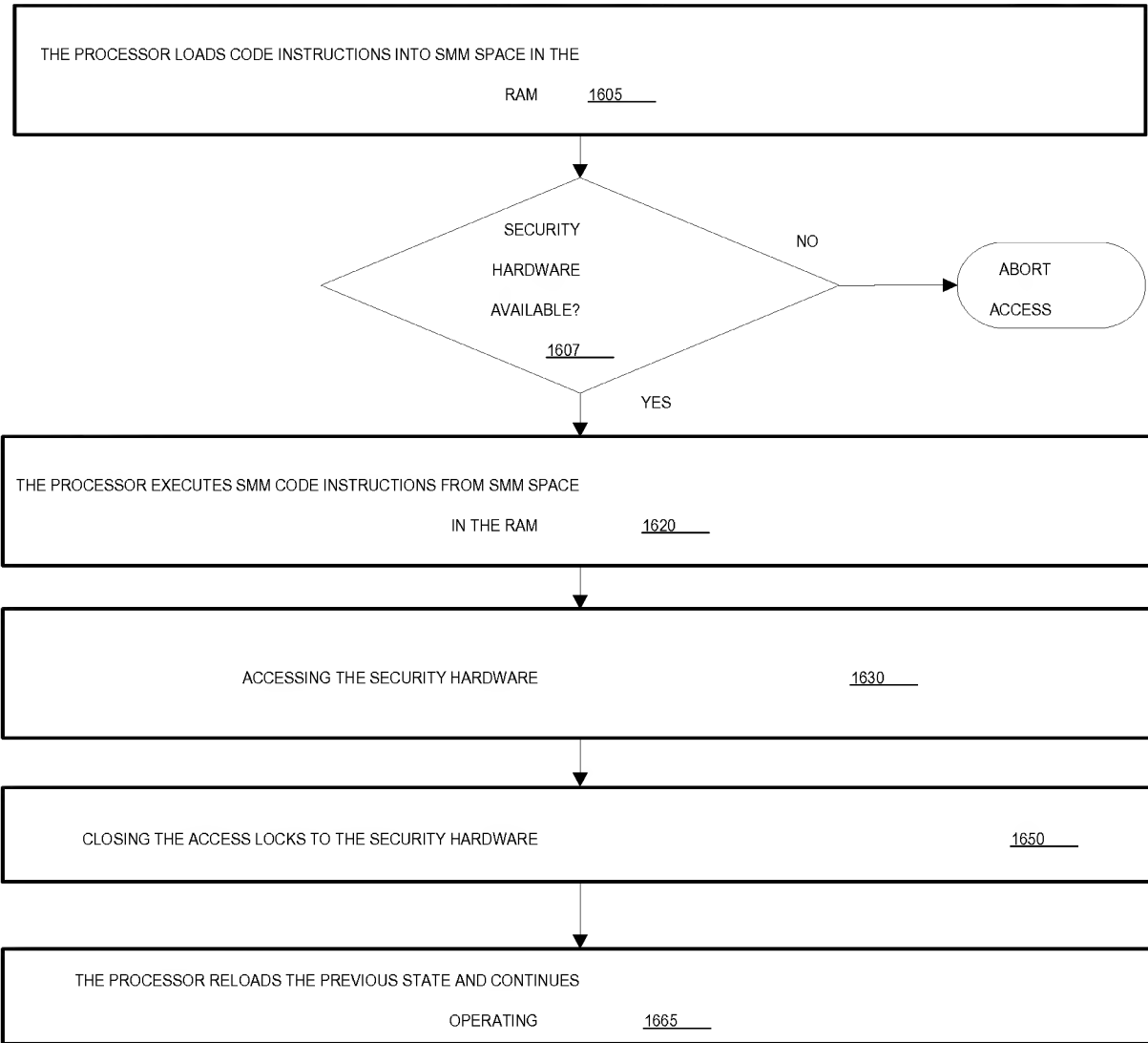


Fig. 16G

1600G

ABORT
ACCESS

1630

1650

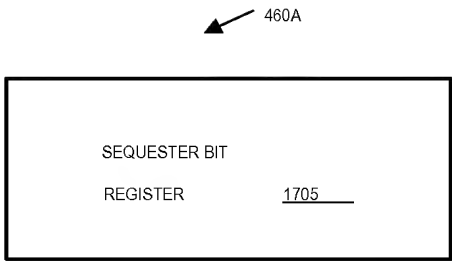


Fig. 17A



Fig. 17B

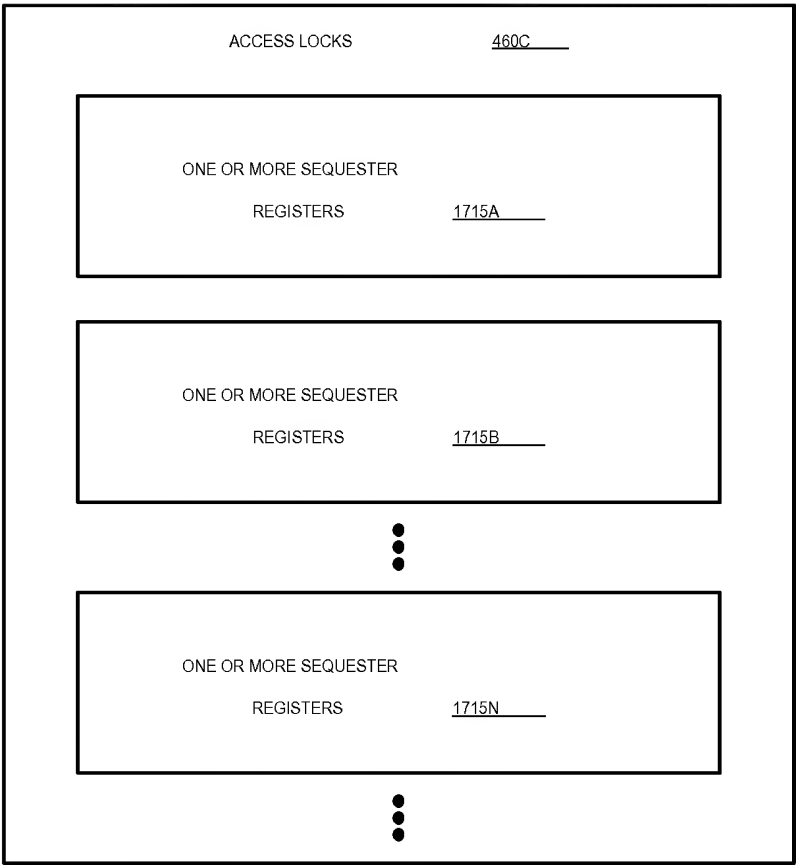


Fig. 17C

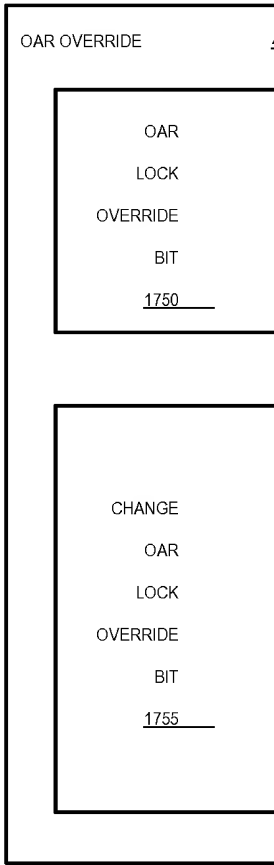
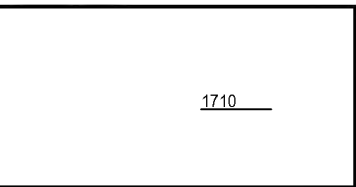


Fig. 17D

460B



7B

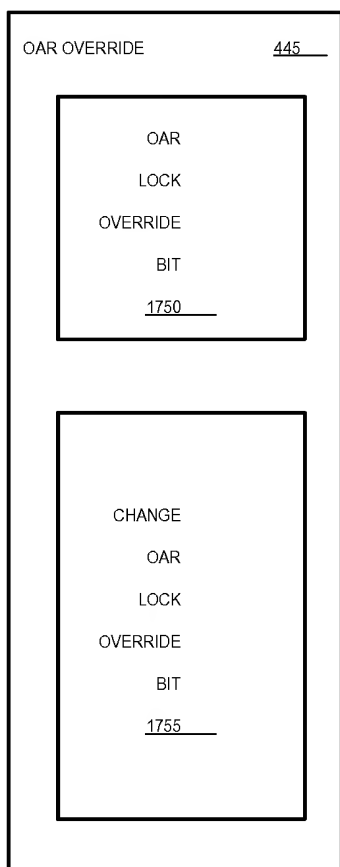


Fig. 17D

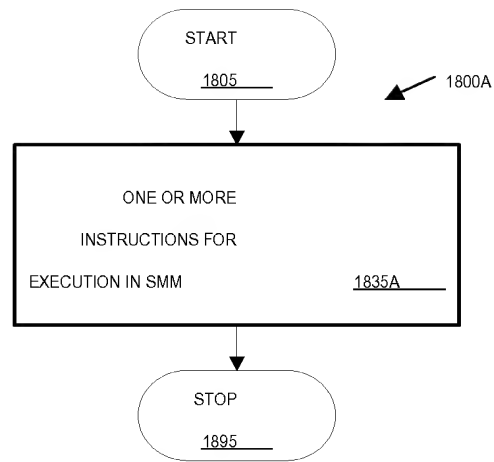


Fig. 18A
PRIOR ART

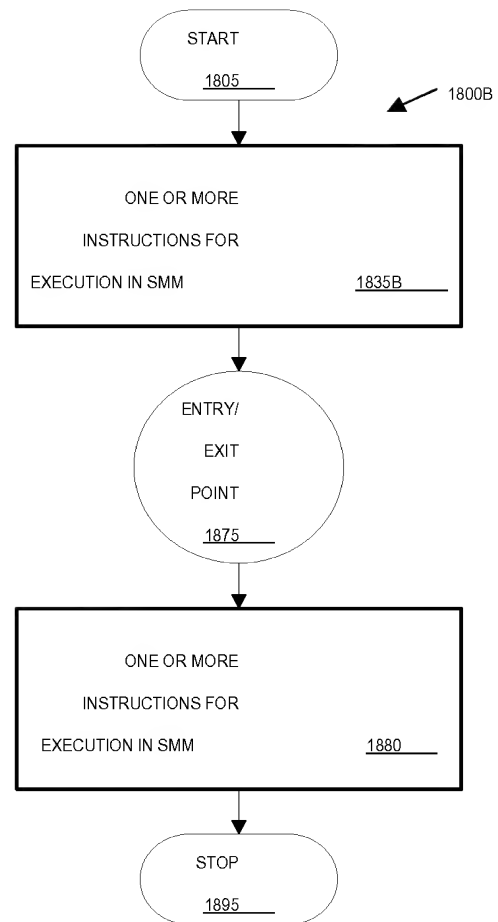
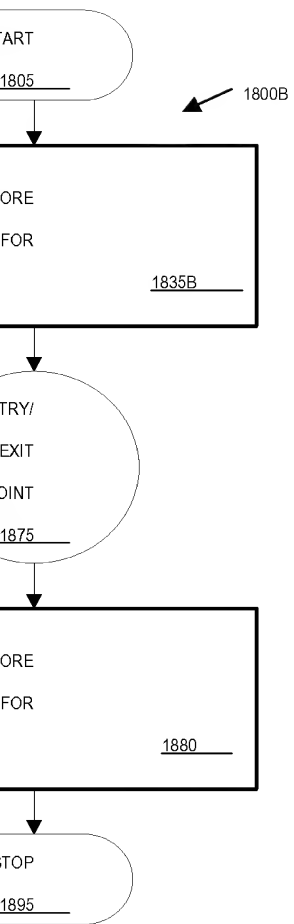


Fig. 18B



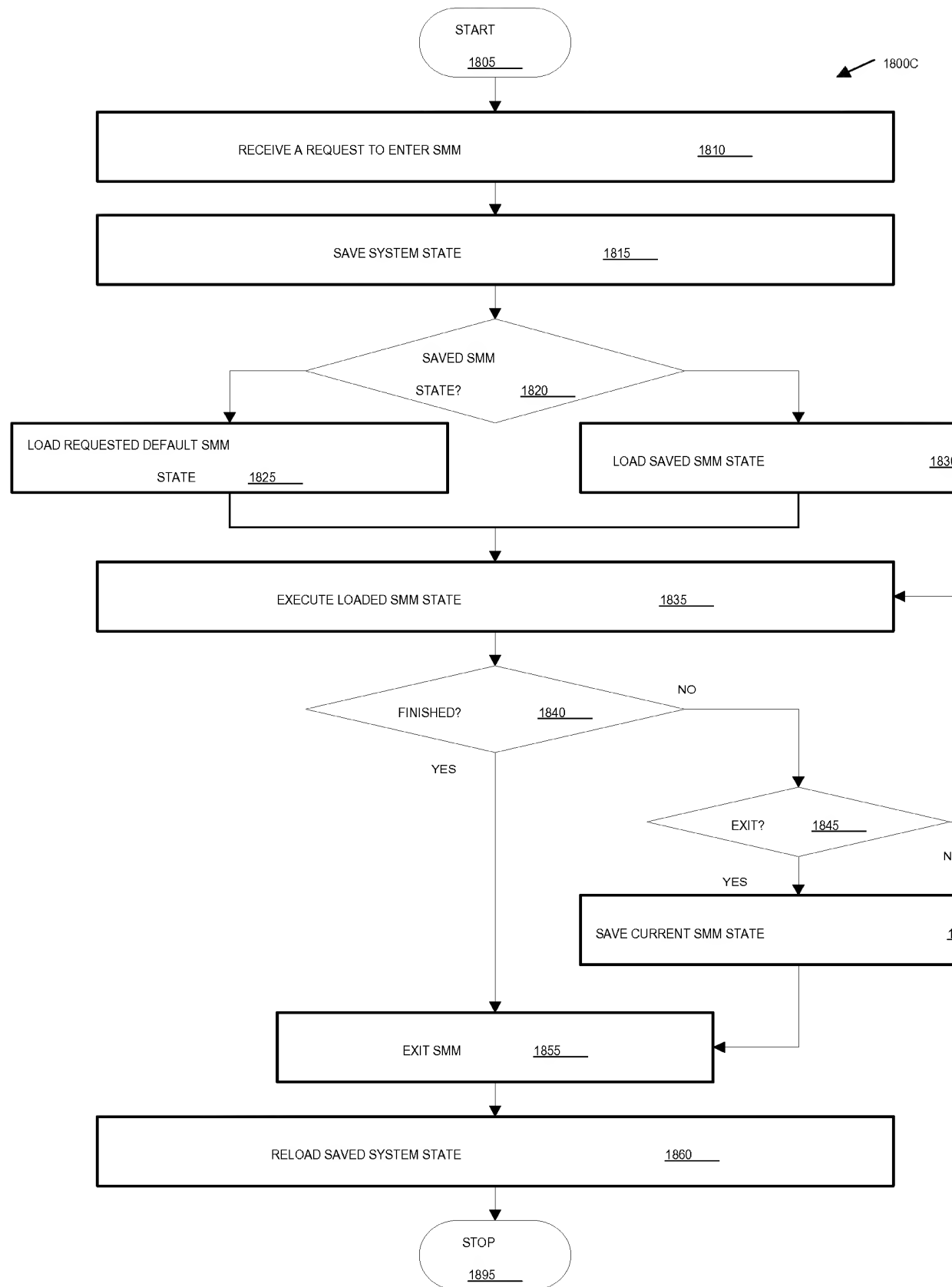


Fig. 18C

1800C

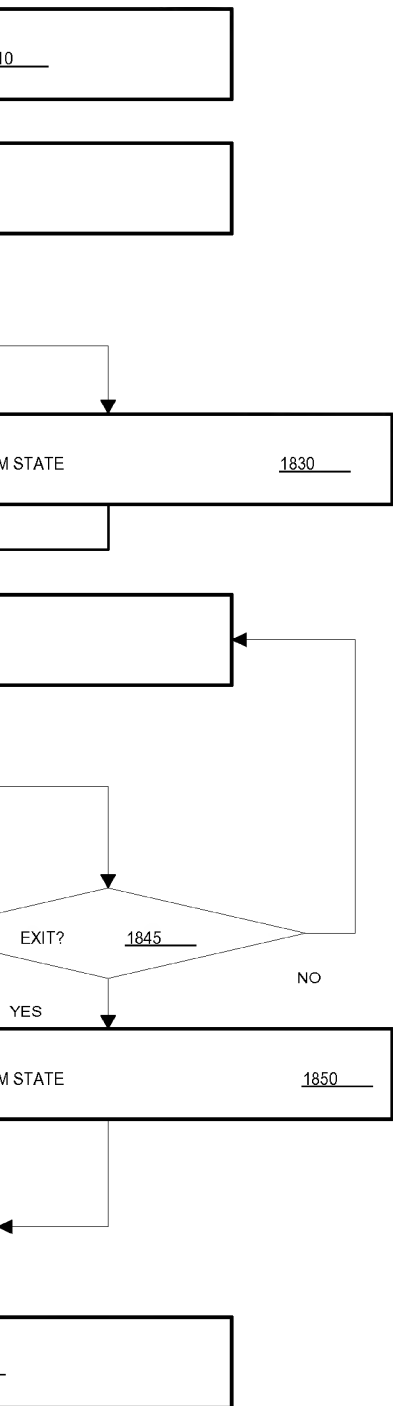


Fig. 18C

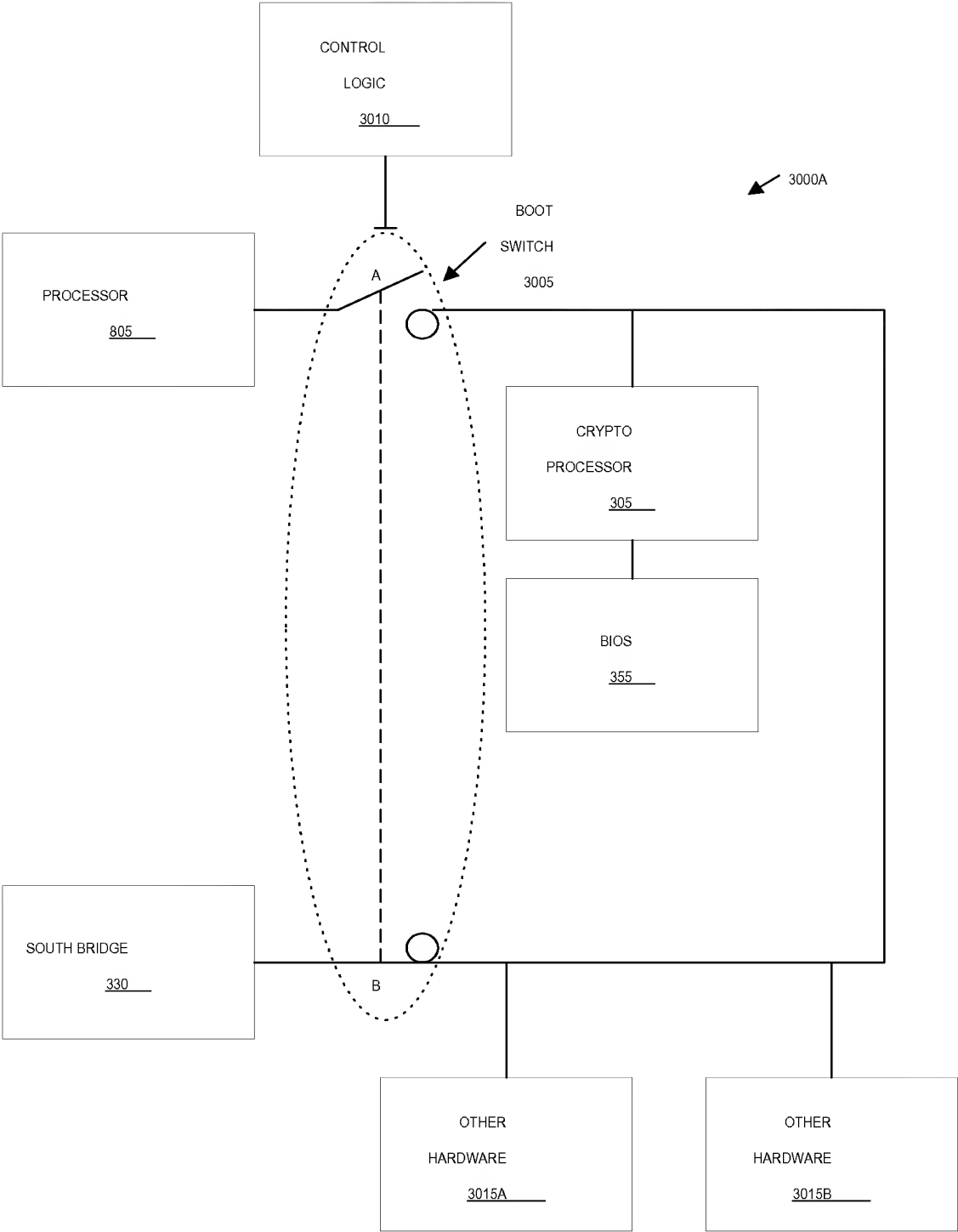
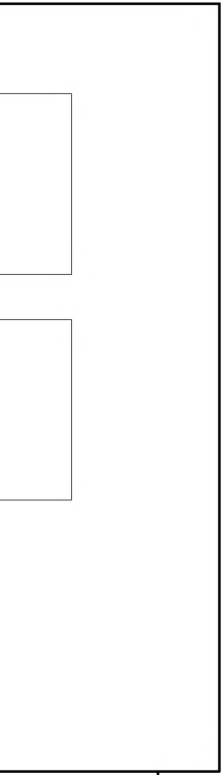


Fig. 19A

3000A



OTHER
HARDWARE

3015B

3000B →

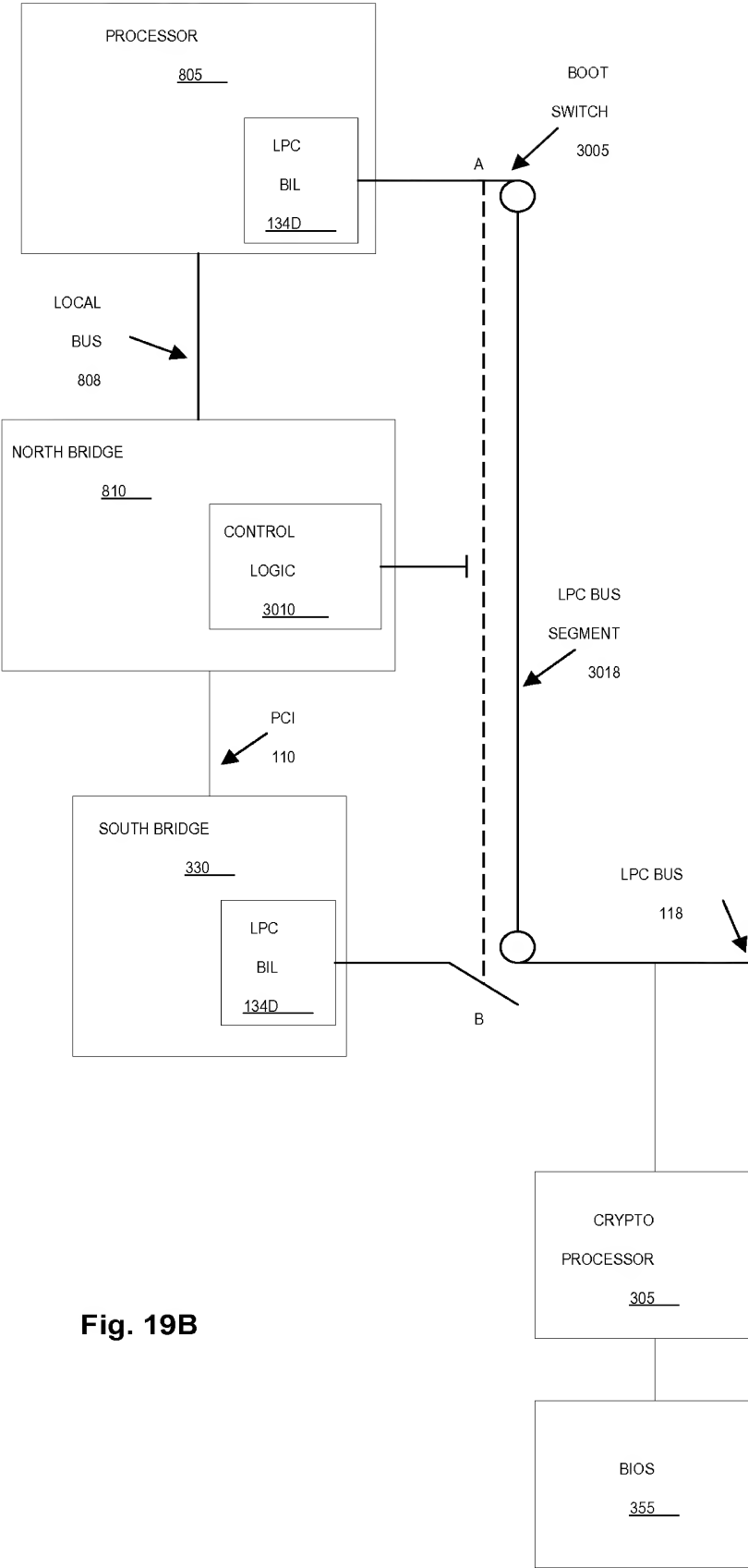
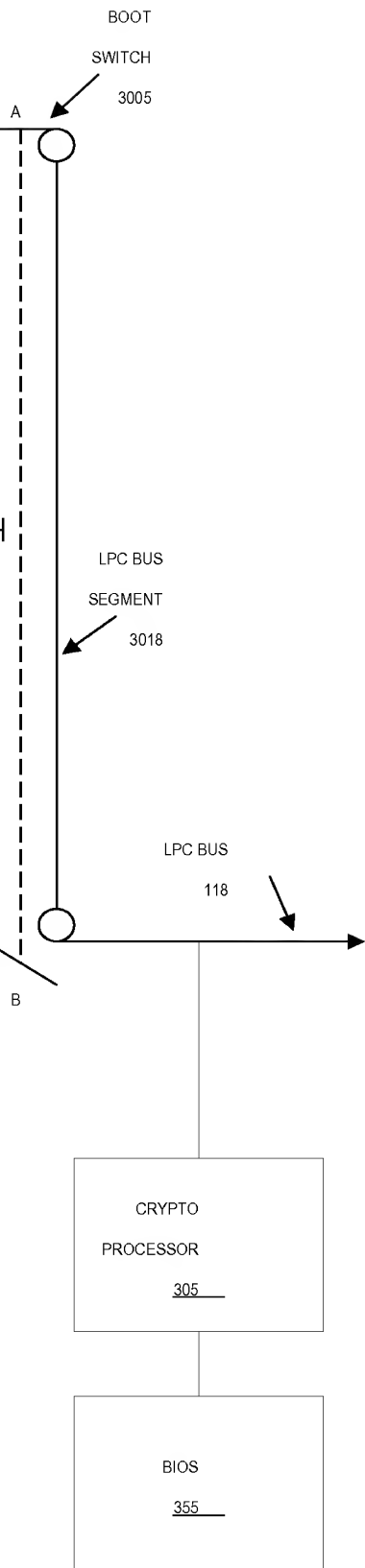


Fig. 19B



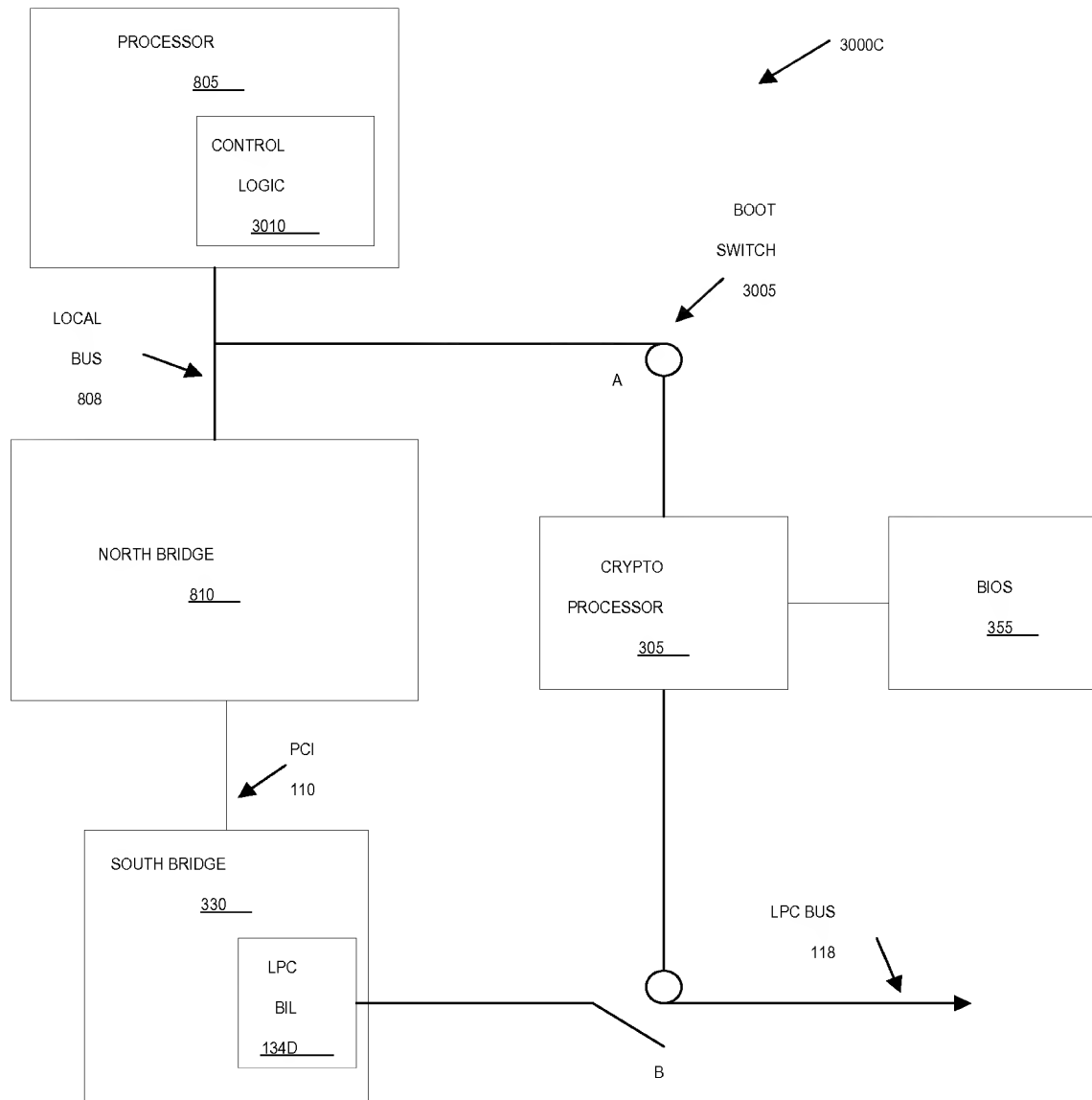
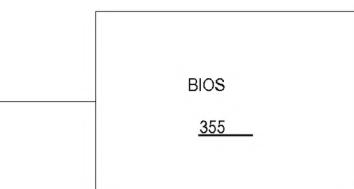


Fig. 19C

3000C



BUS



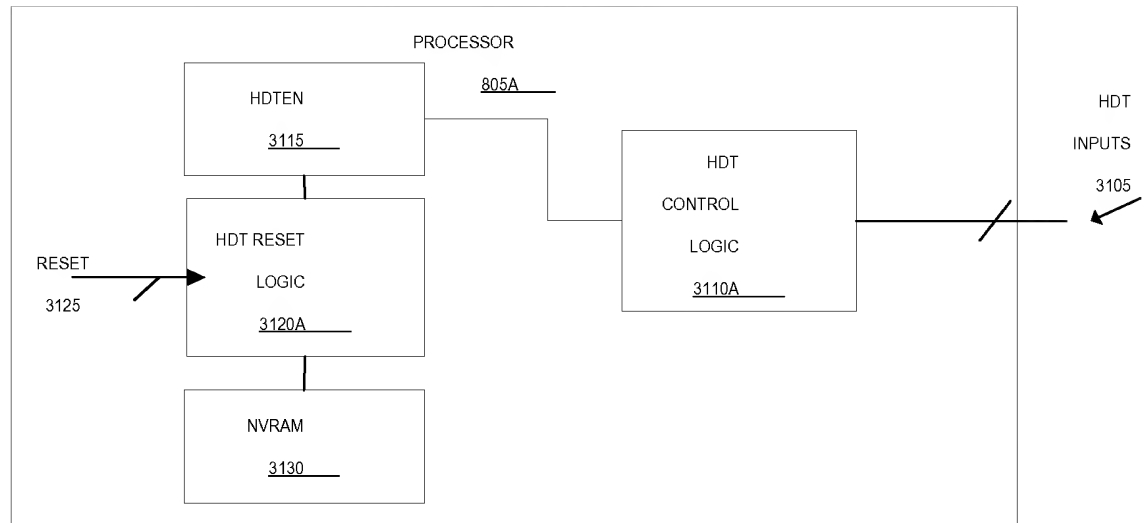


Fig. 20A

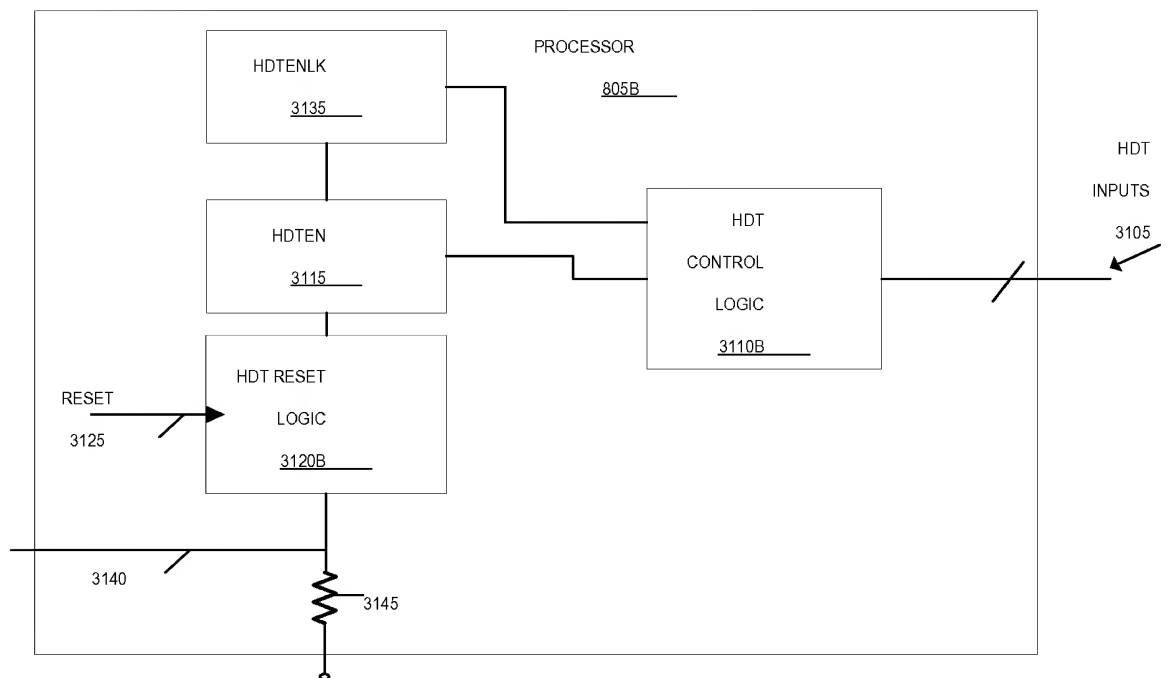
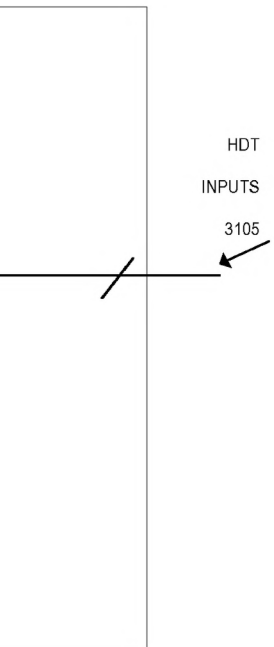
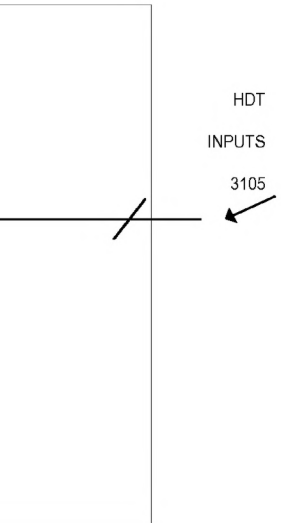
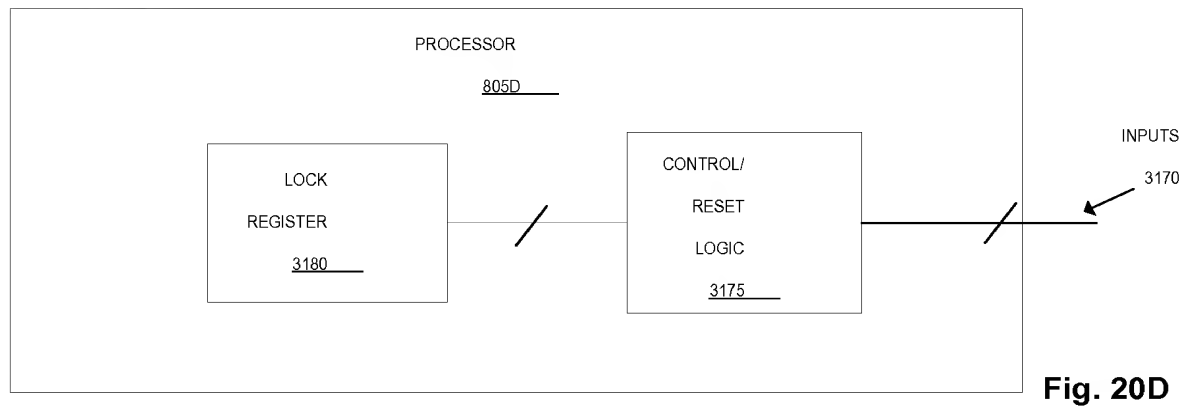
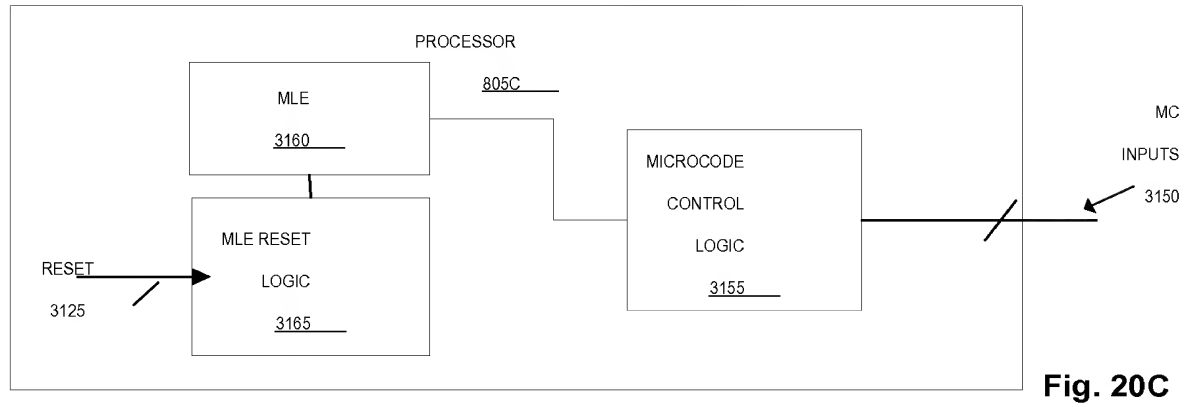
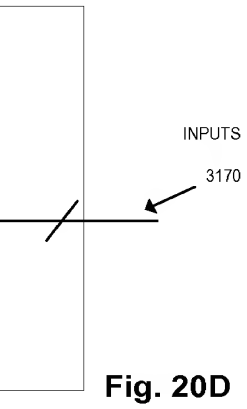
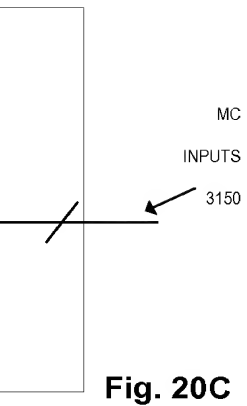
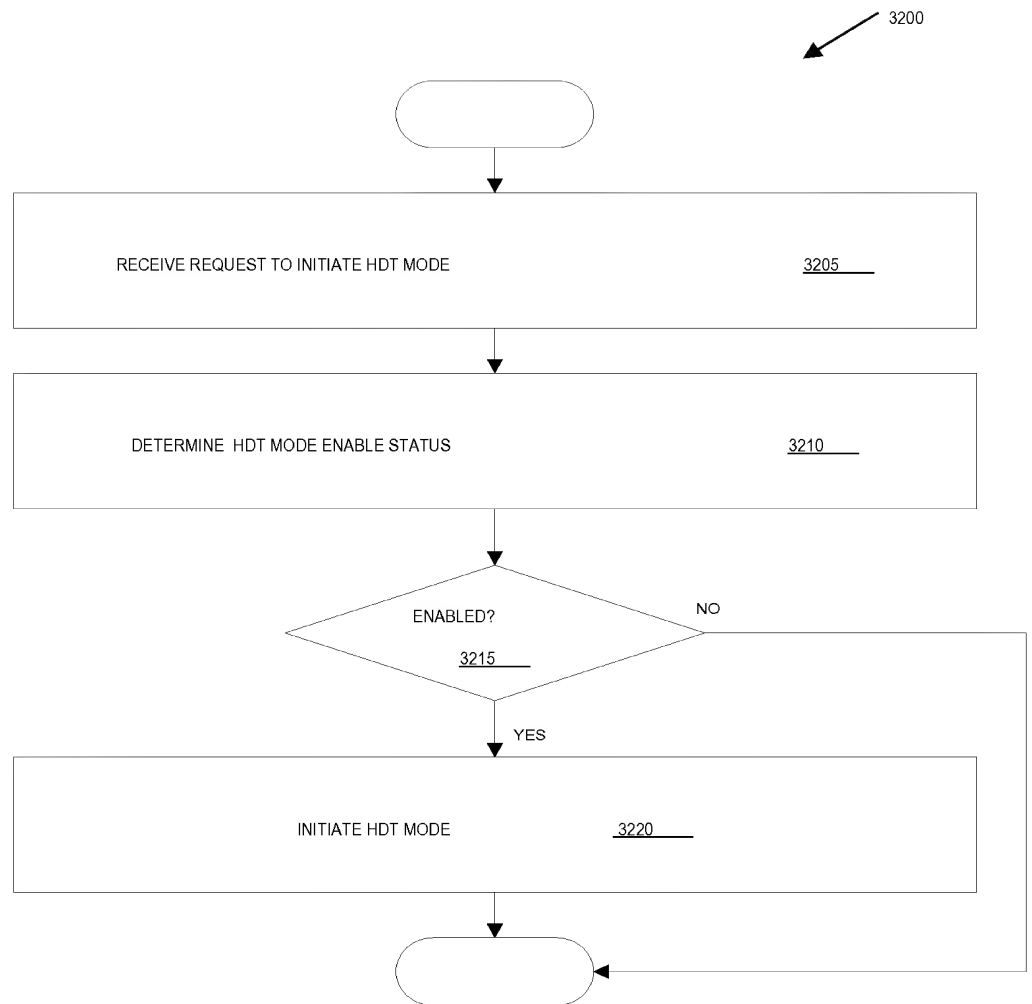


Fig. 20B







**Fig. 21**

3200

205

0

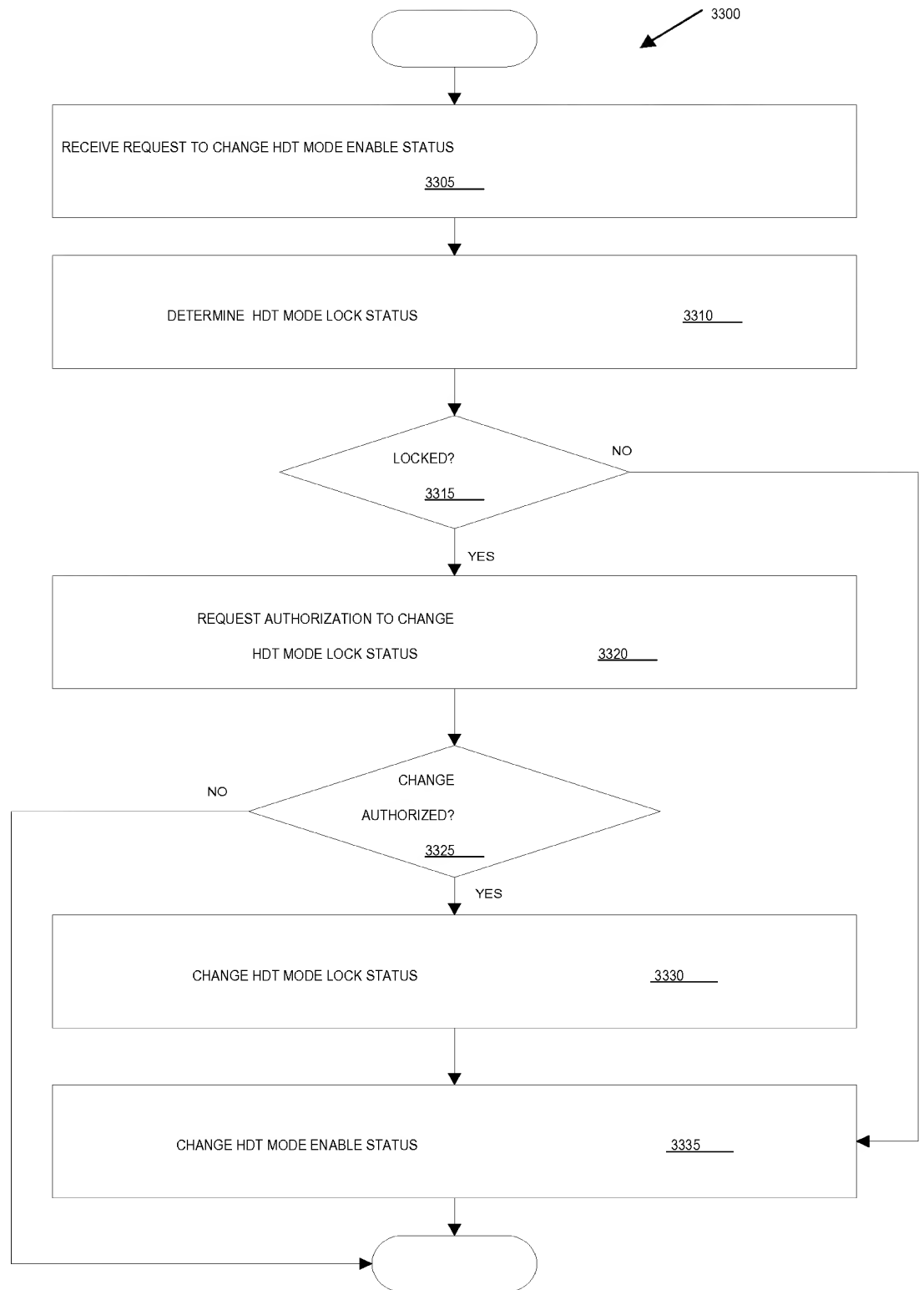
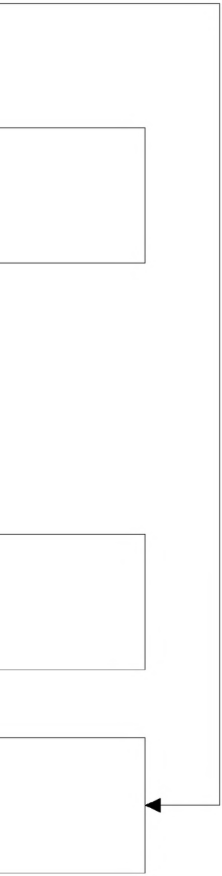
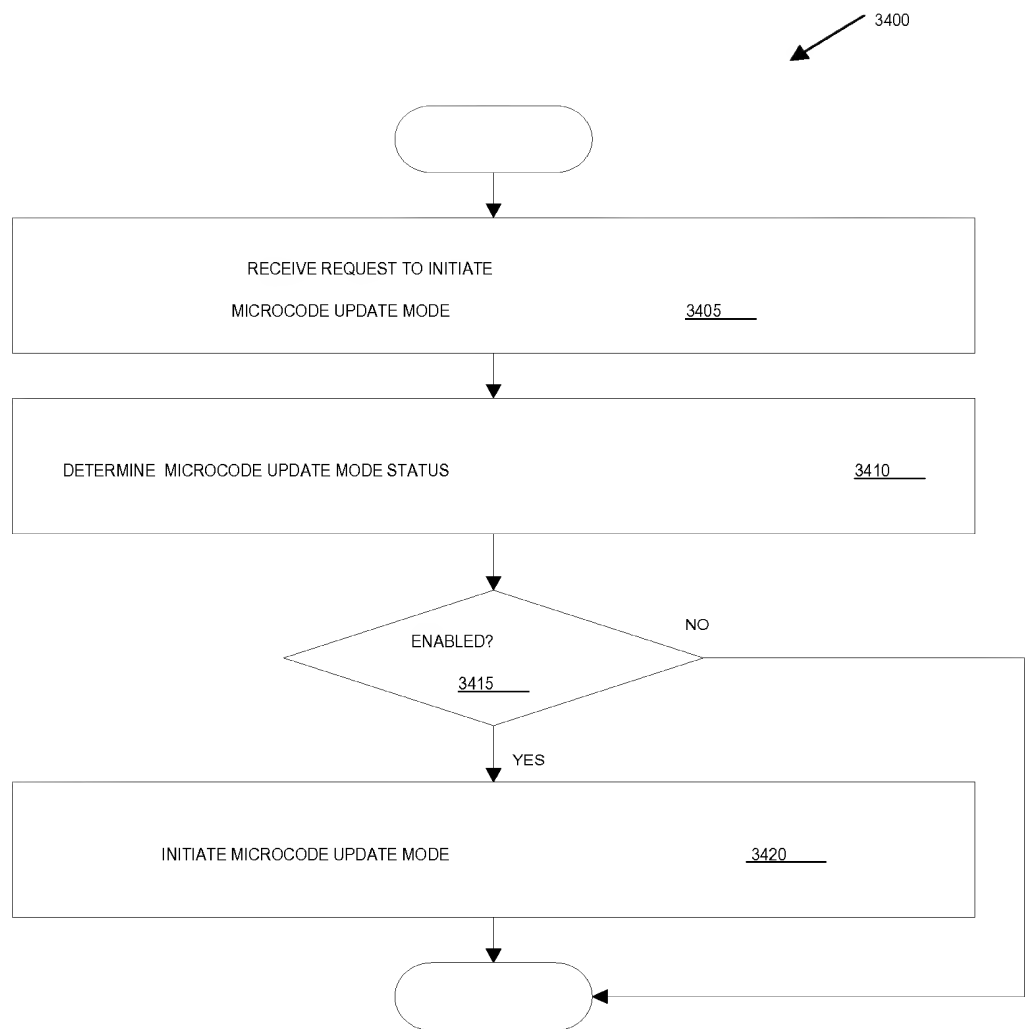


Fig. 22

-



**Fig. 23**

3400

3410

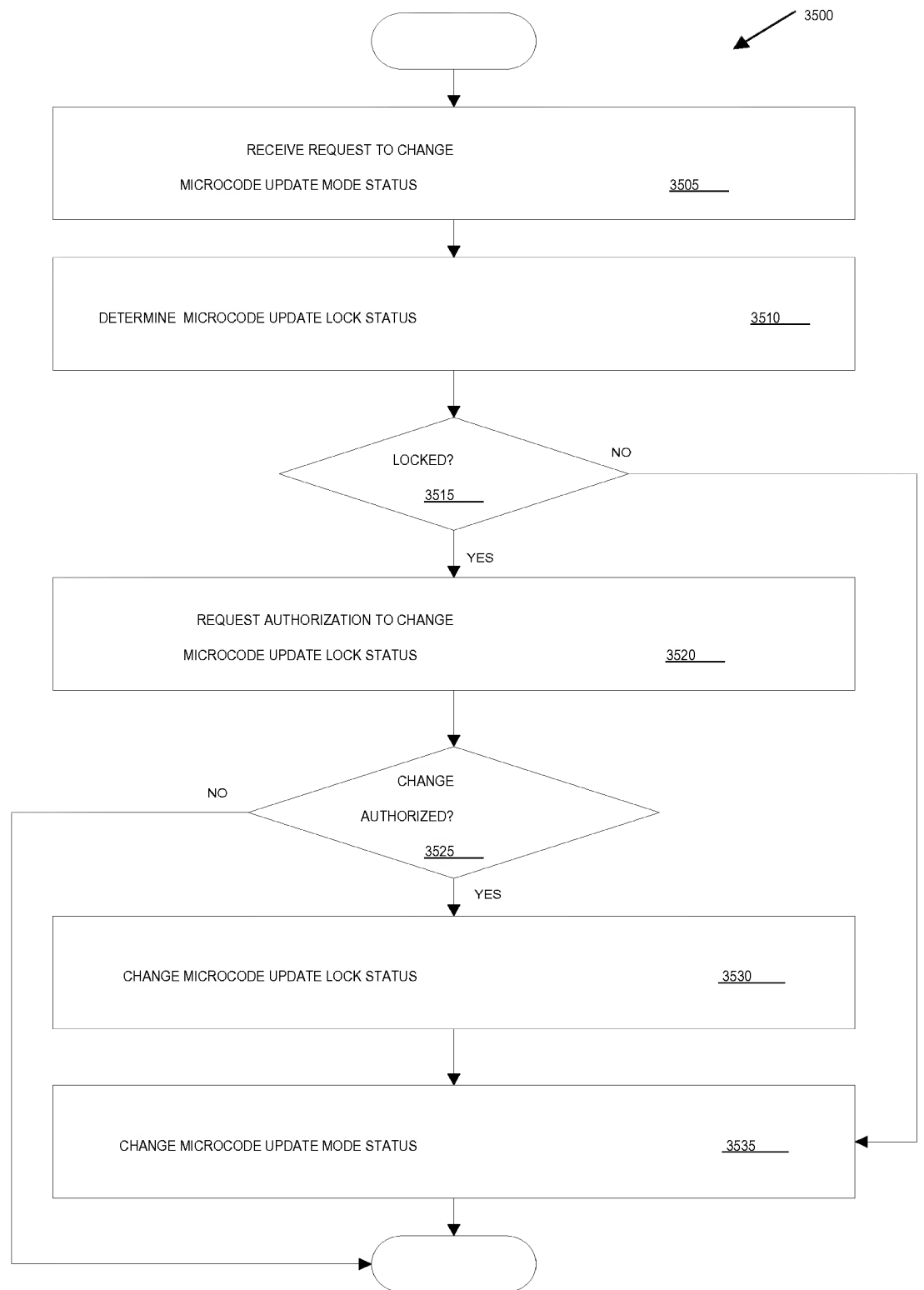
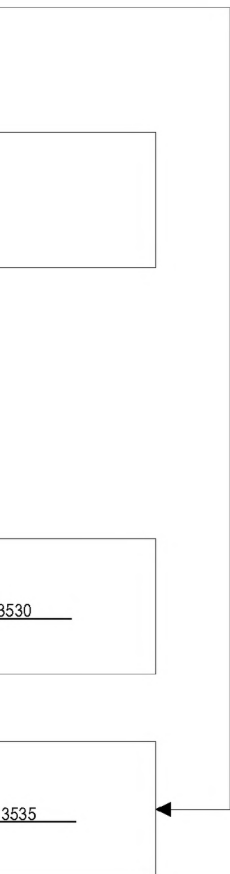


Fig. 24

3500

-

3510



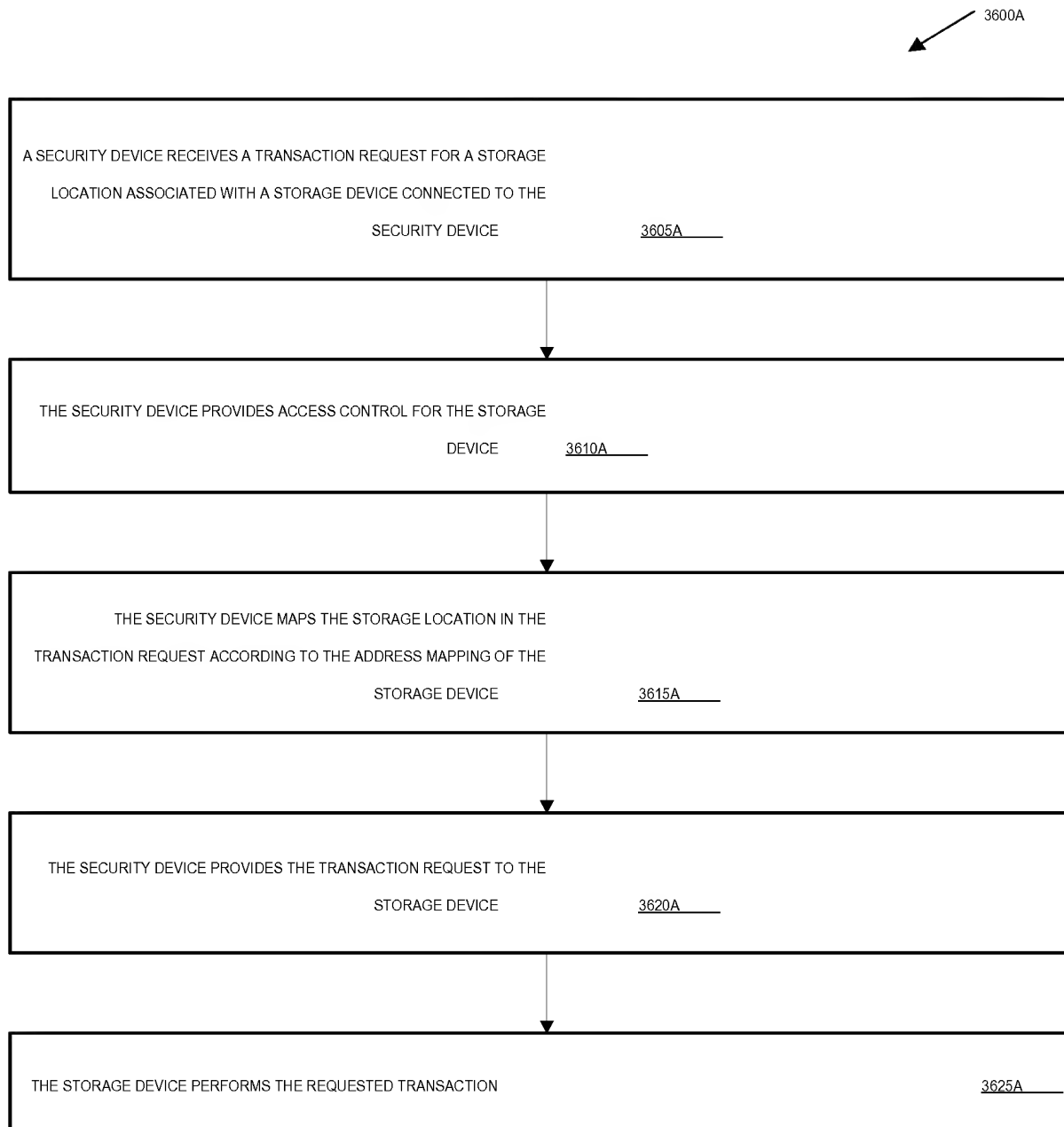


Fig. 25A

3600A



--

--

--

--

3625A

--

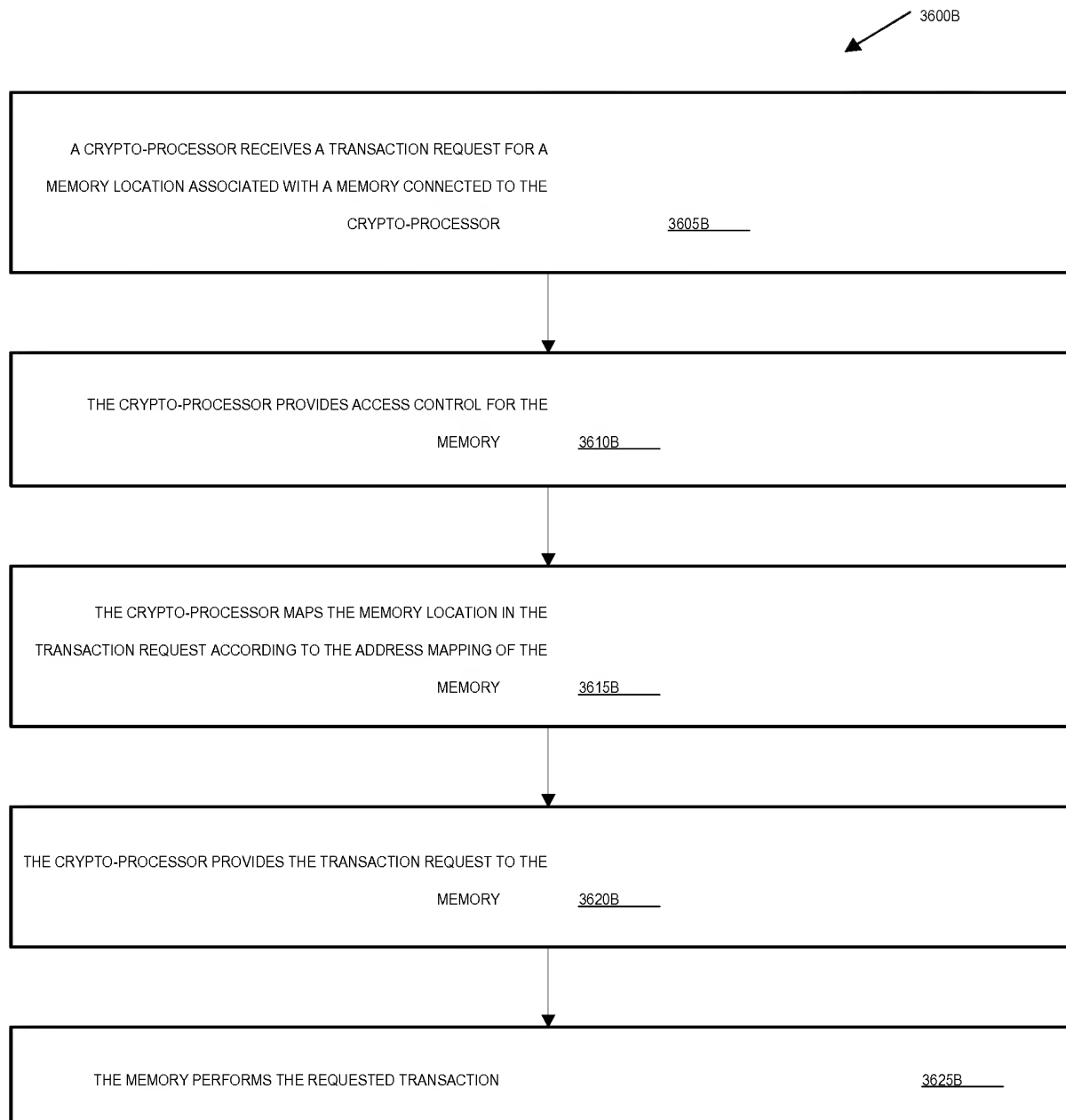


Fig. 25B

3600B

3625B

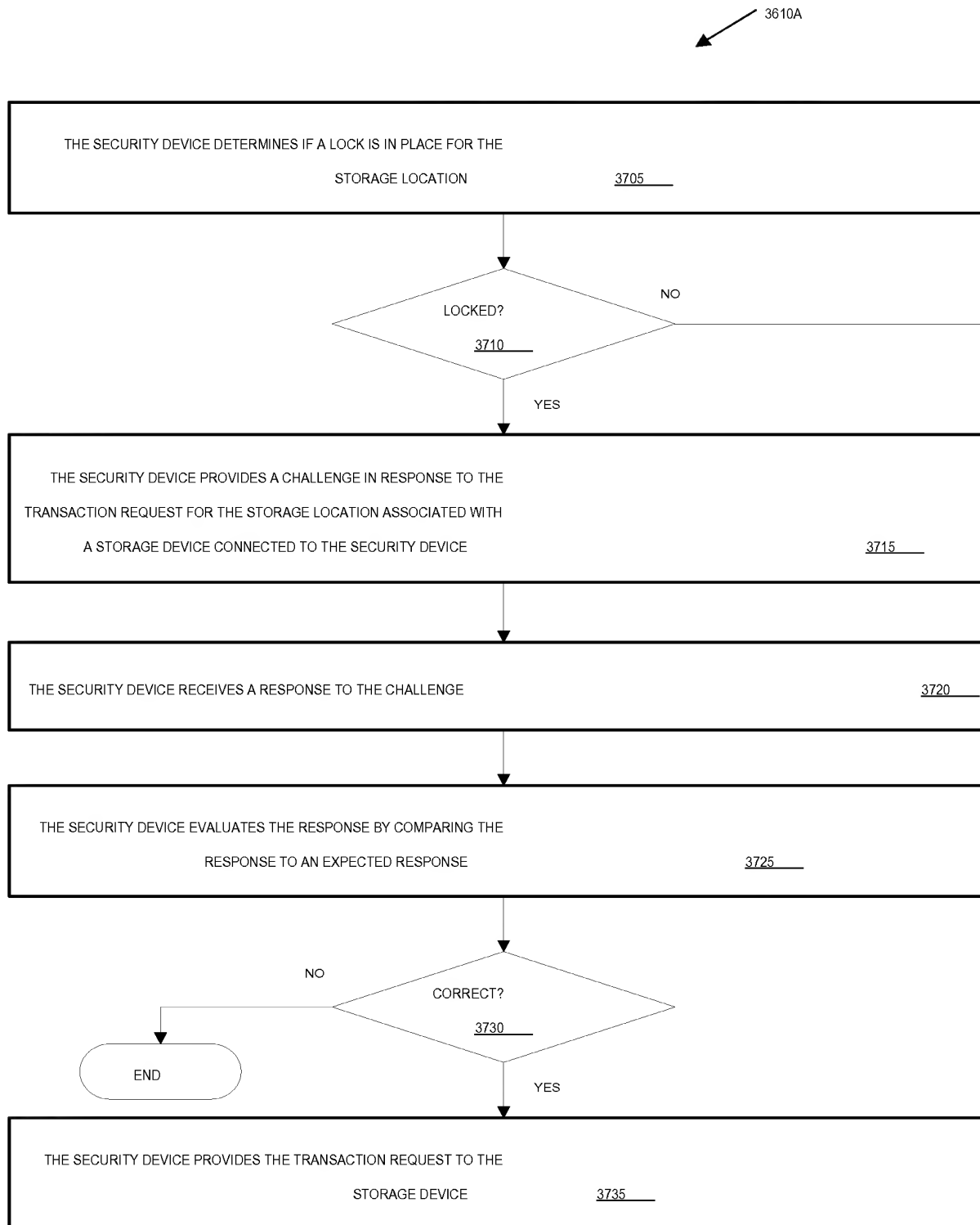


Fig. 26

3610A

3715

3720

3725

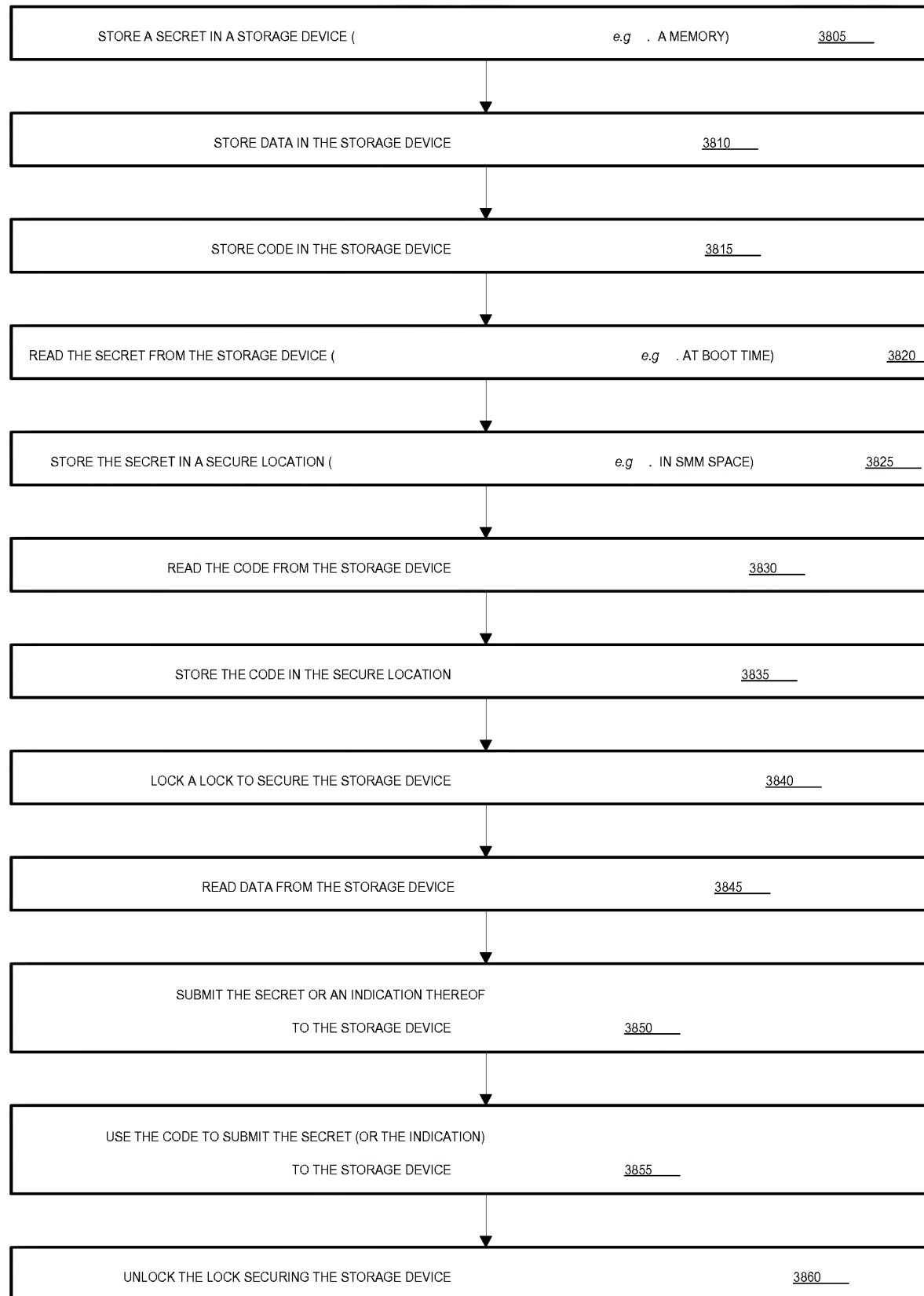


Fig. 27

3620

EMORY)	<u>3805</u>
--------	-------------

<u>3810</u>

<u>3815</u>

AT BOOT TIME)	<u>3820</u>
---------------	-------------

MM SPACE)	<u>3825</u>
-----------	-------------

<u>3830</u>

<u>3835</u>

<u>3840</u>

<u>3845</u>

--

--

<u>3860</u>

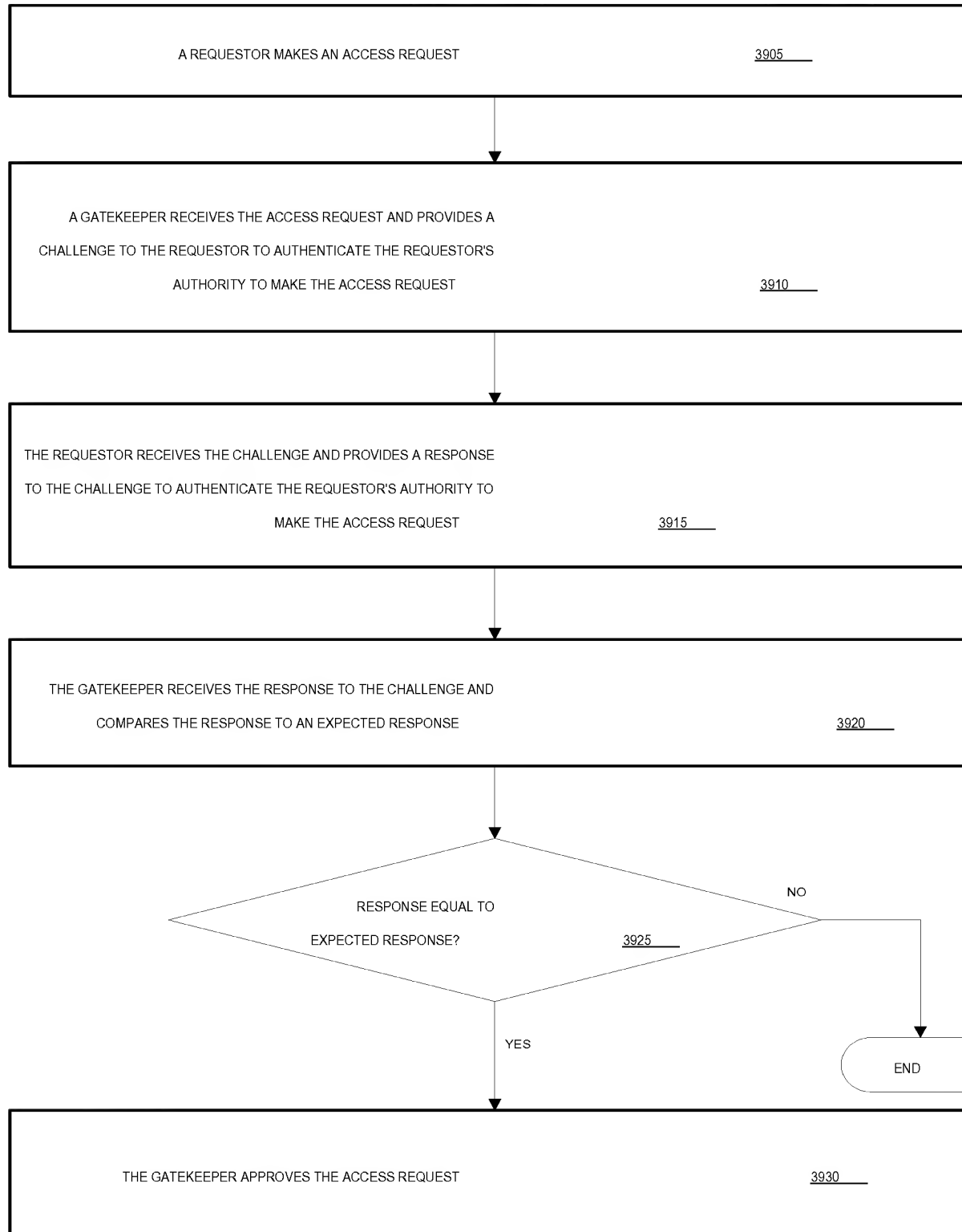


Fig. 28
(Prior Art)

3900

3905

3910

3920

NO

END

3930

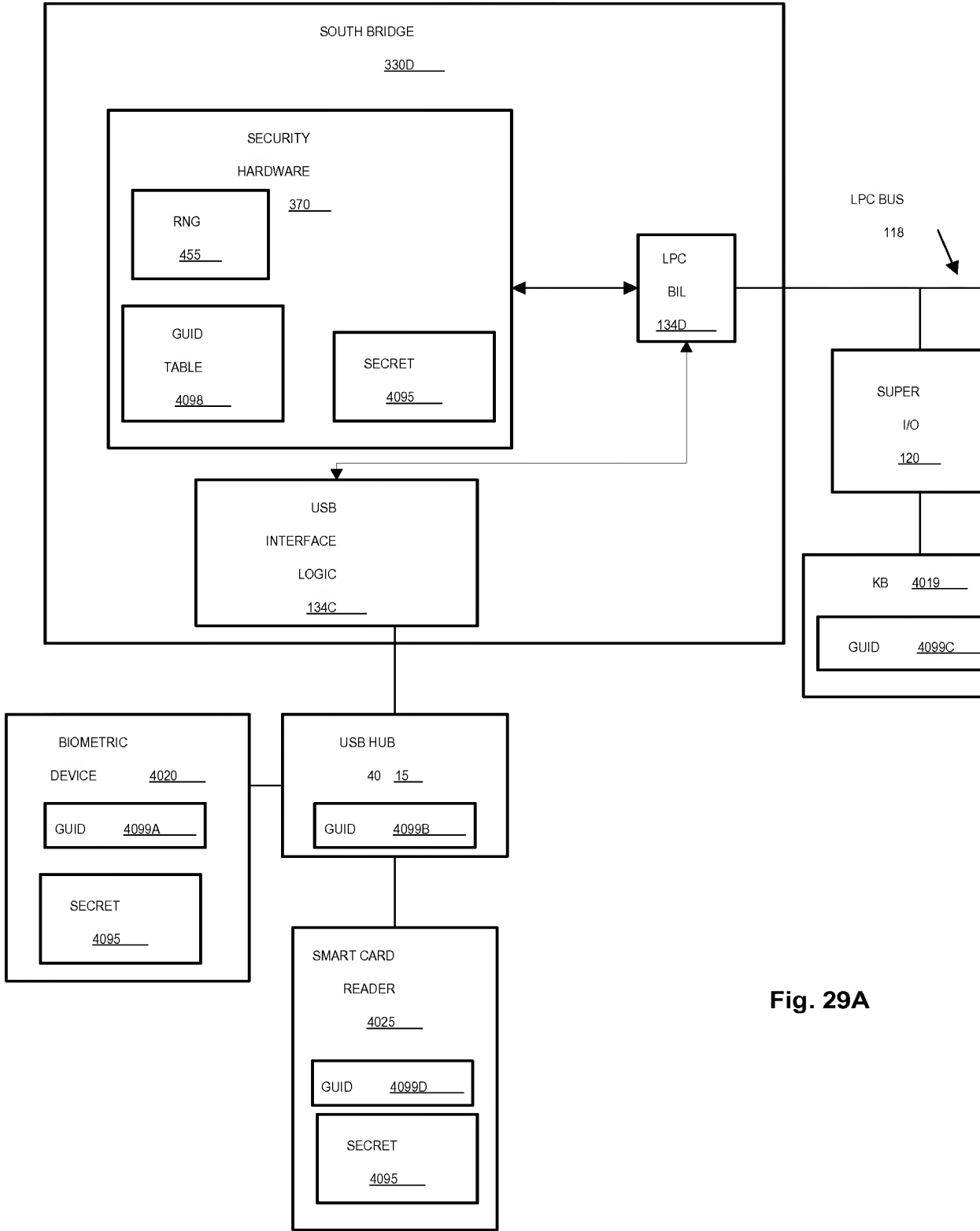


Fig. 29A

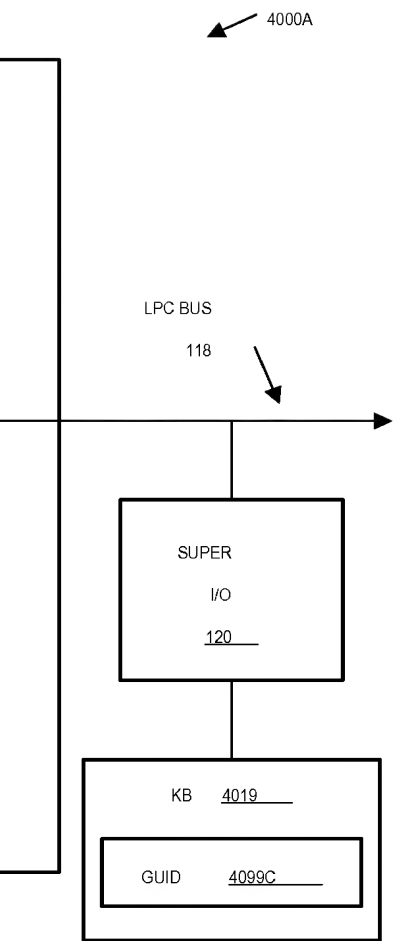


Fig. 29A

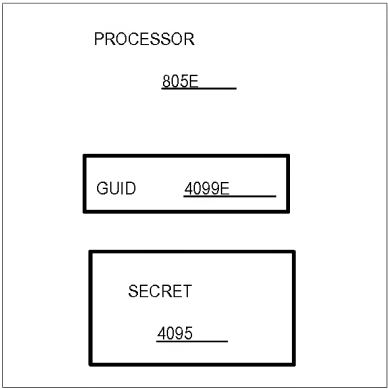


Fig. 29B

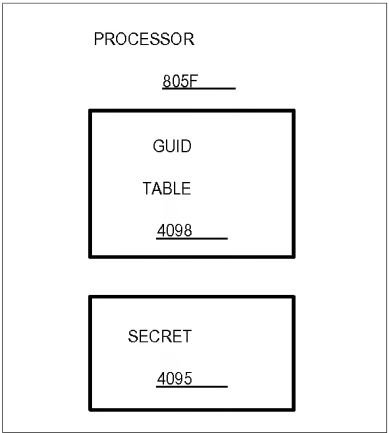


Fig. 29C

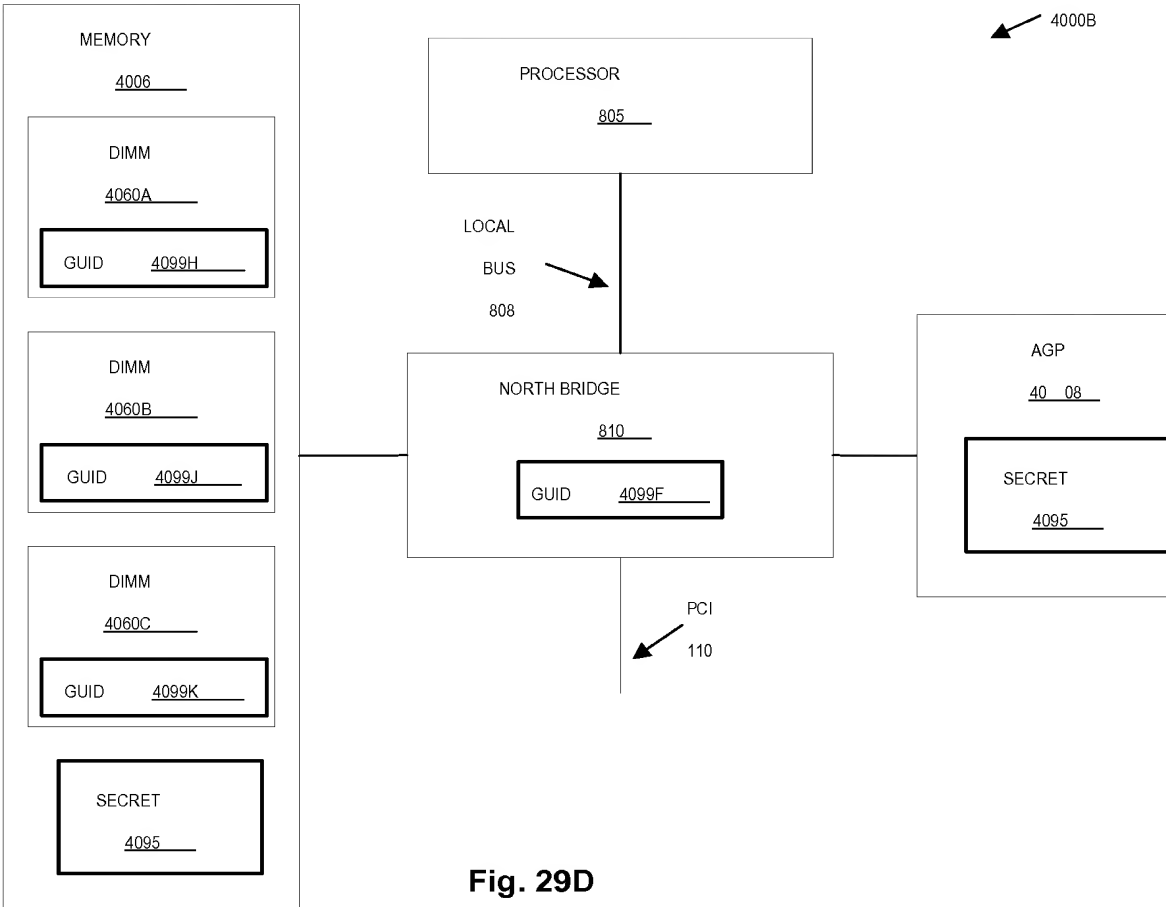


Fig. 29D

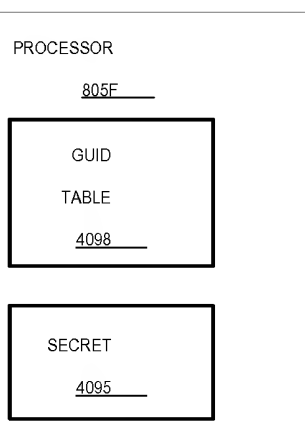
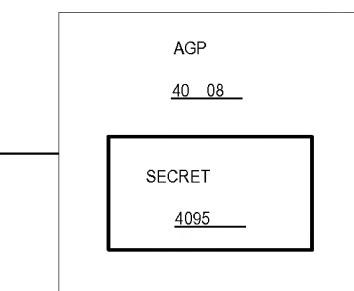


Fig. 29C

4000B

An arrow points from the text '4000B' to the left, towards the center of the page.



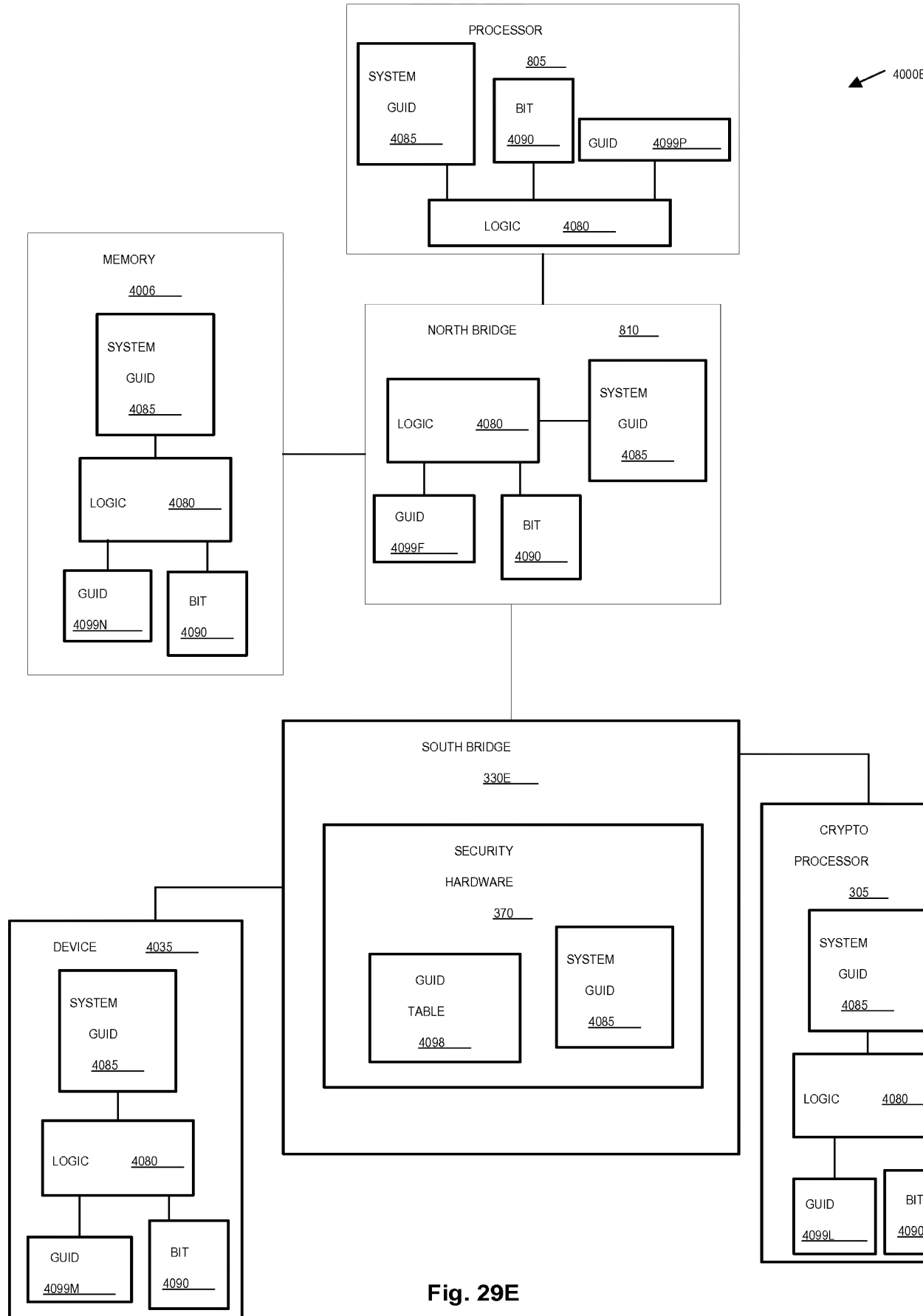
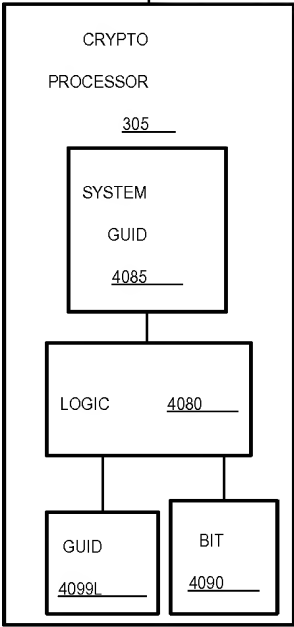


Fig. 29E

4000E



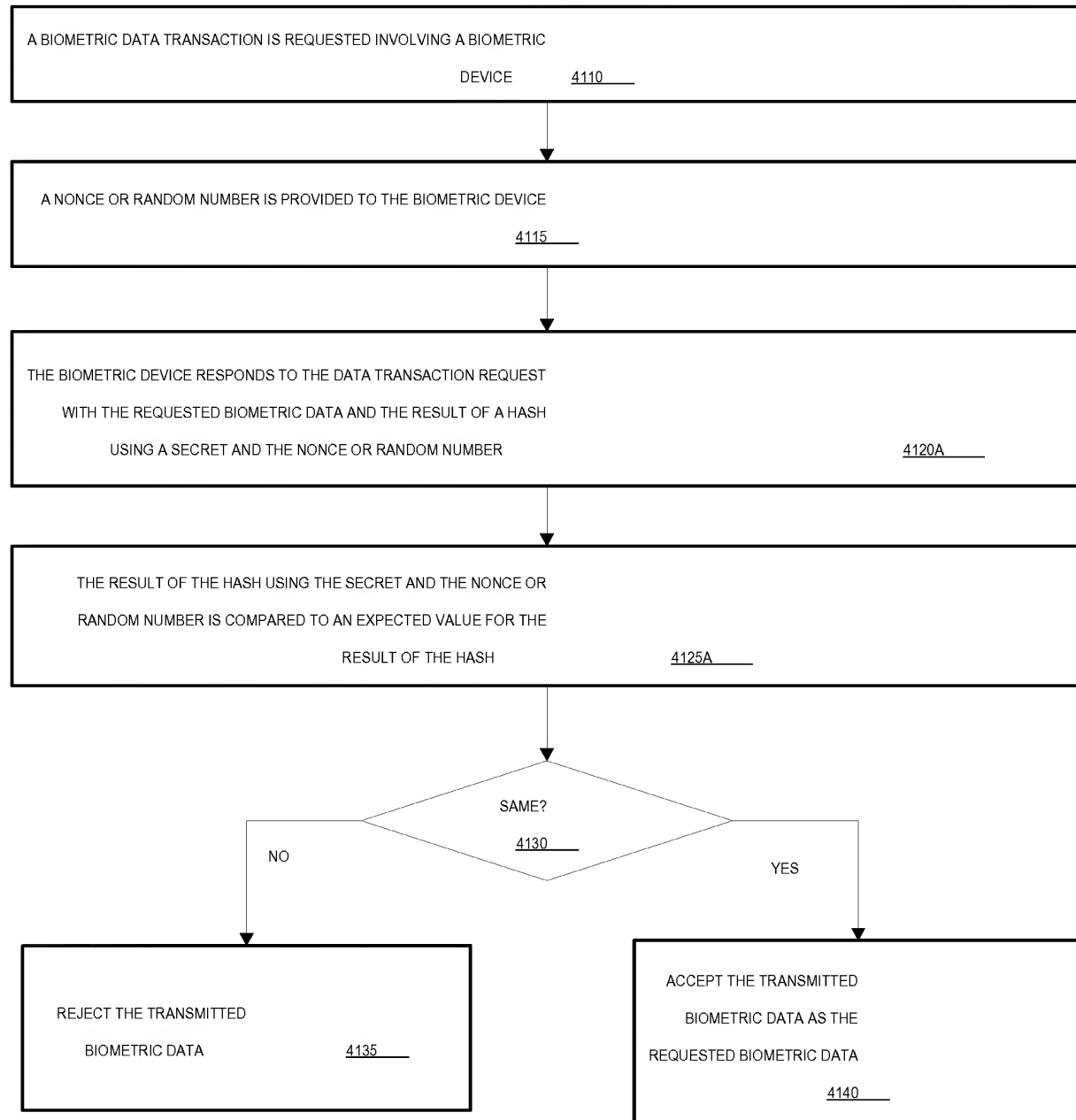


Fig. 30A

4100A

4120A

RTED
THE
DATA
4140

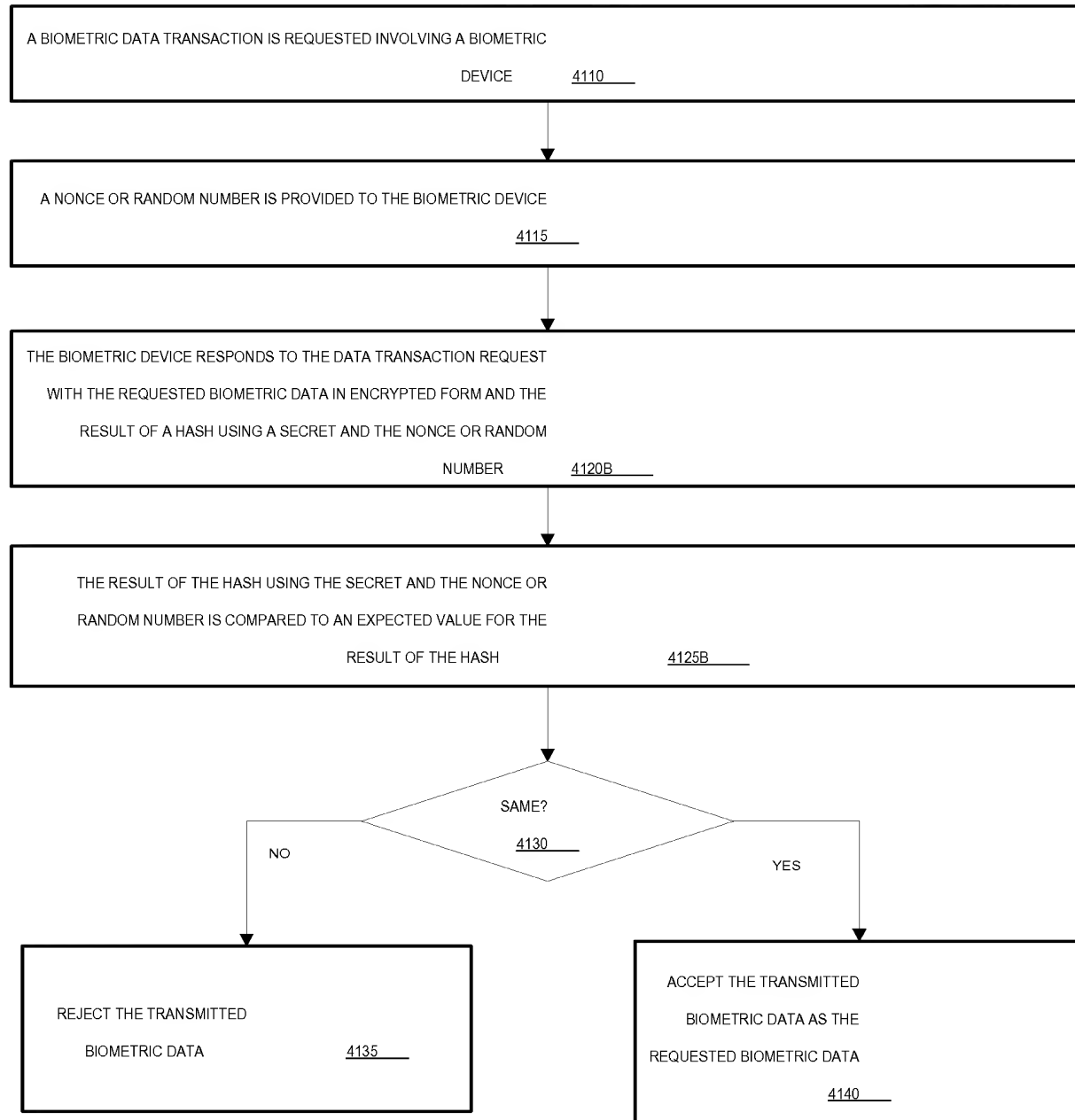


Fig. 30B

4100B

SMITTED
AS THE
IC DATA
4140

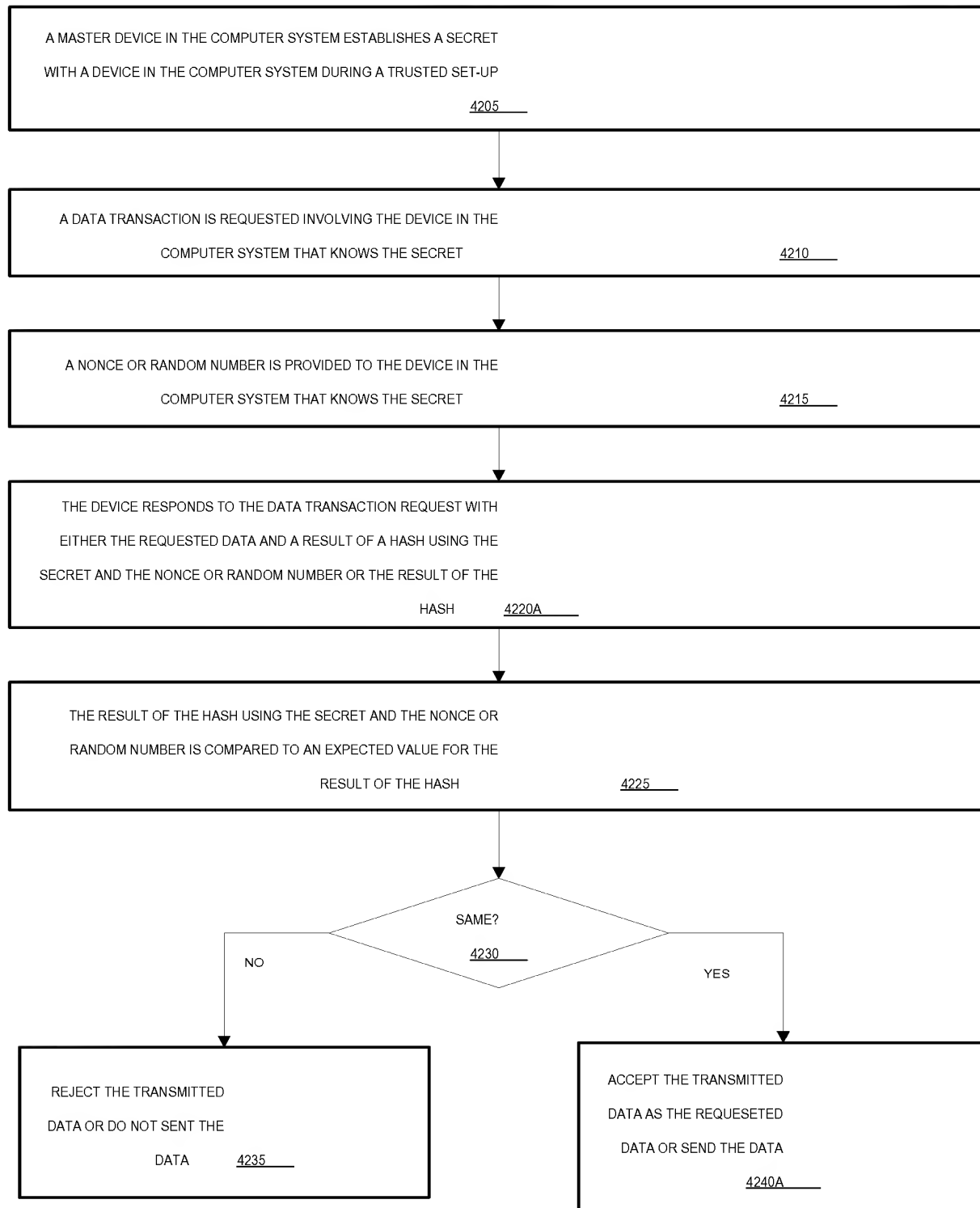


Fig. 31A

4200A

4210

4215

SMITTED
ESETED
HE DATA
4240A

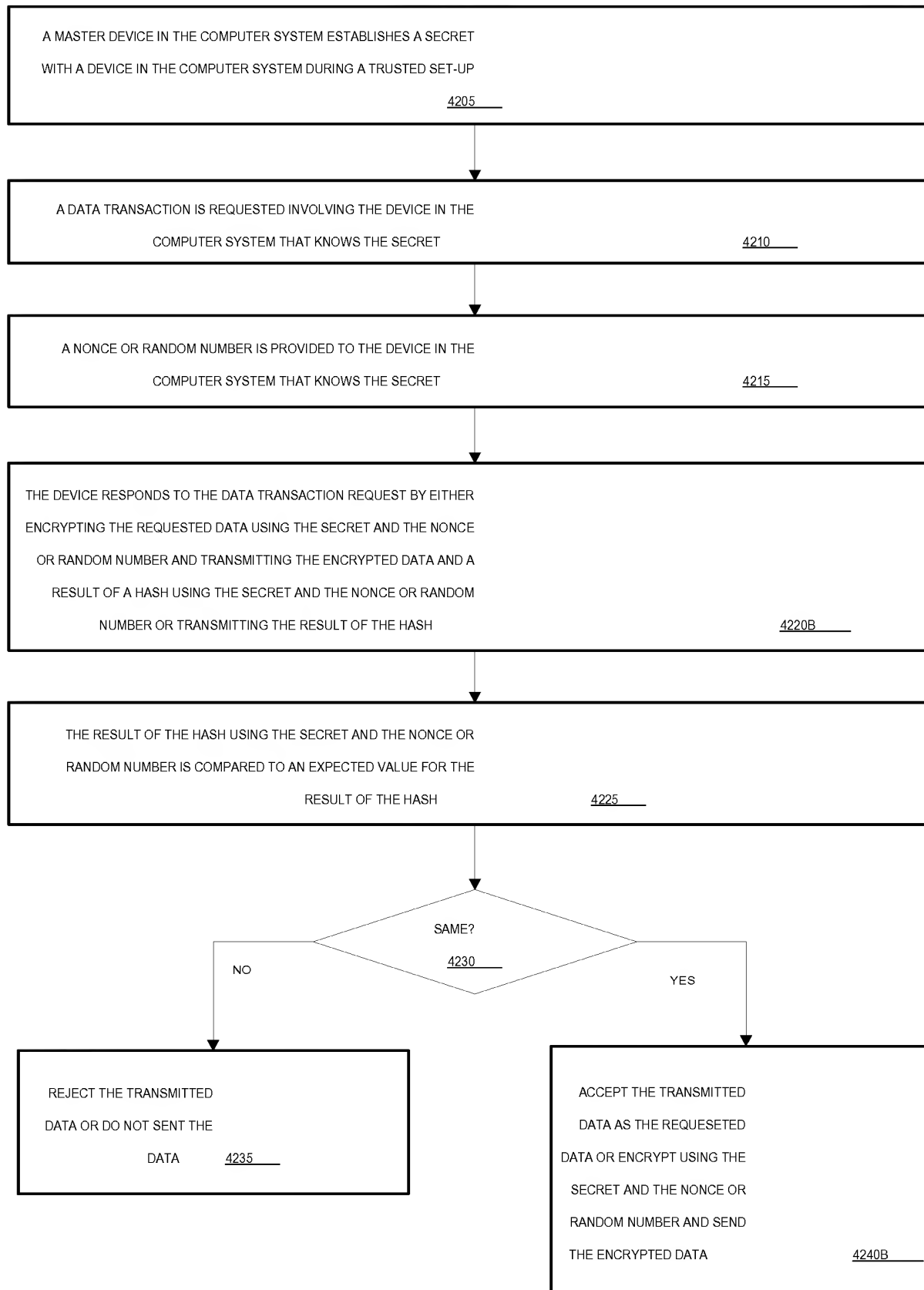


Fig. 31B

4200B

4210

4215

4220B

S

TRANSMITTED
RESETED
USING THE
IONCE OR
AND SEND
ATA

4240B

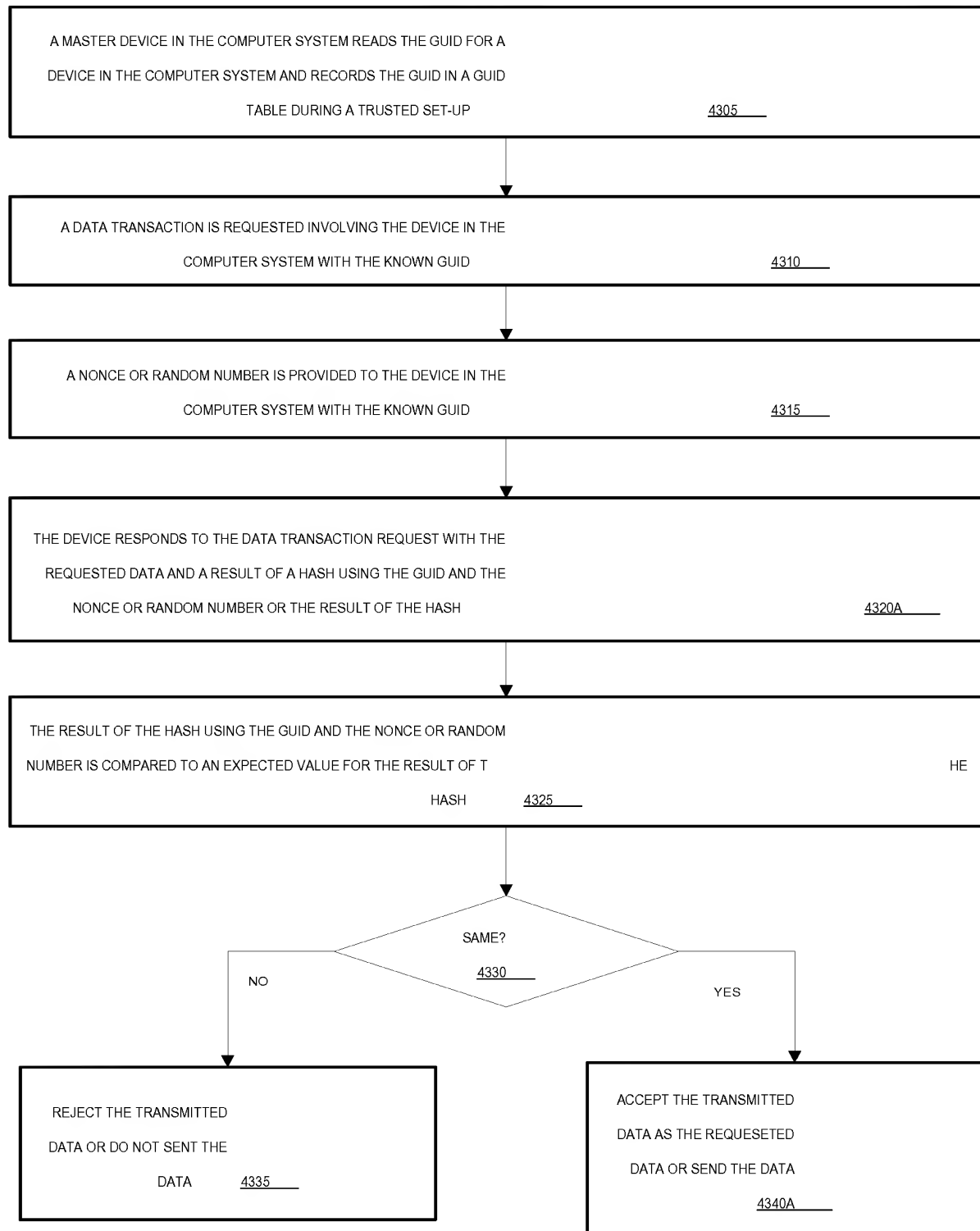


Fig. 32A

4300A

5

4310

4315

4320A

HE

S

TRANSMITTED
QUESETED
THE DATA
4340A

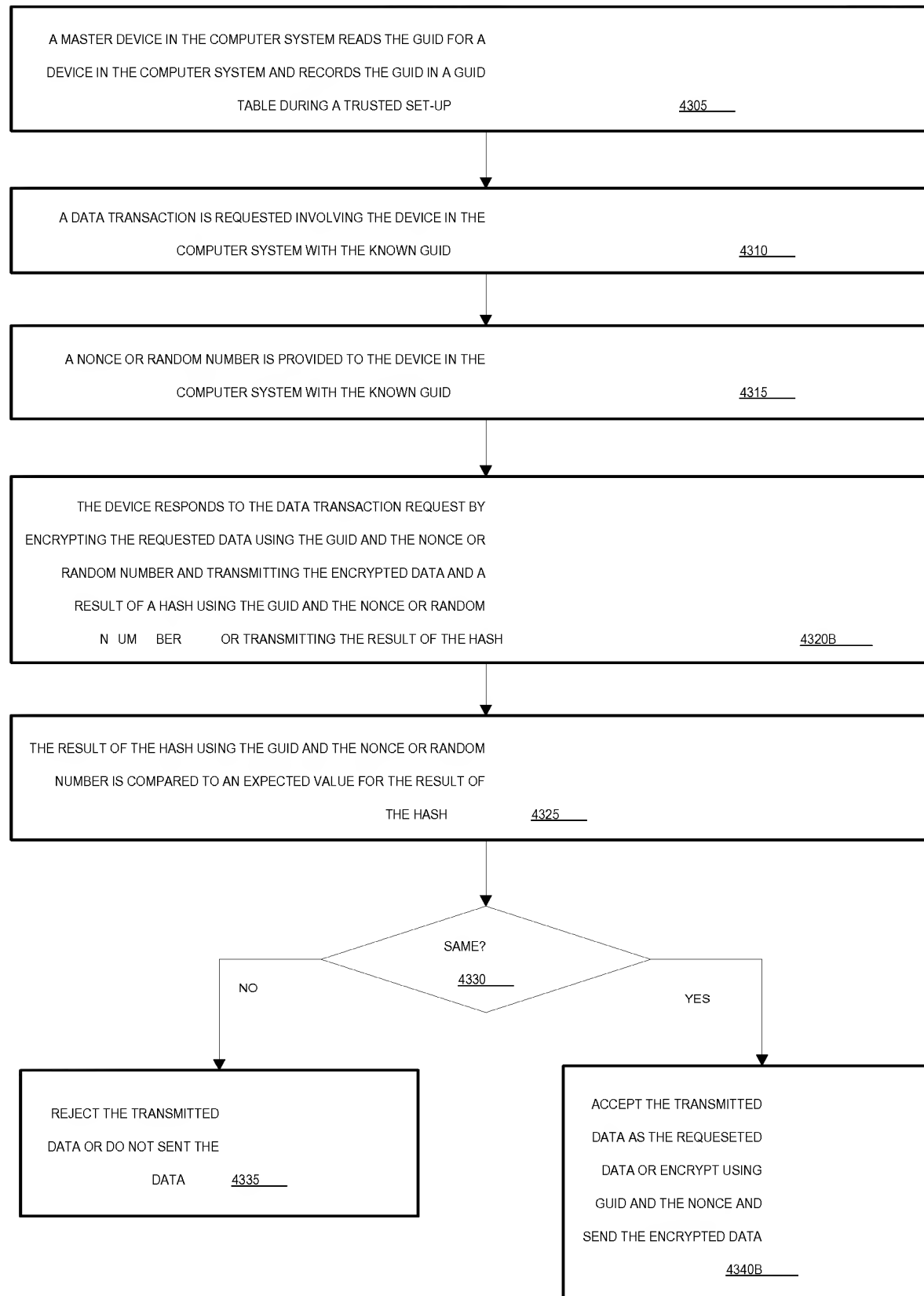


Fig. 32B

4300B

4305

4310

4315

4320B

YES

TRANSMITTED
REQUESTED
CRYPT USING
NONCE AND
CRYPTED DATA

4340B

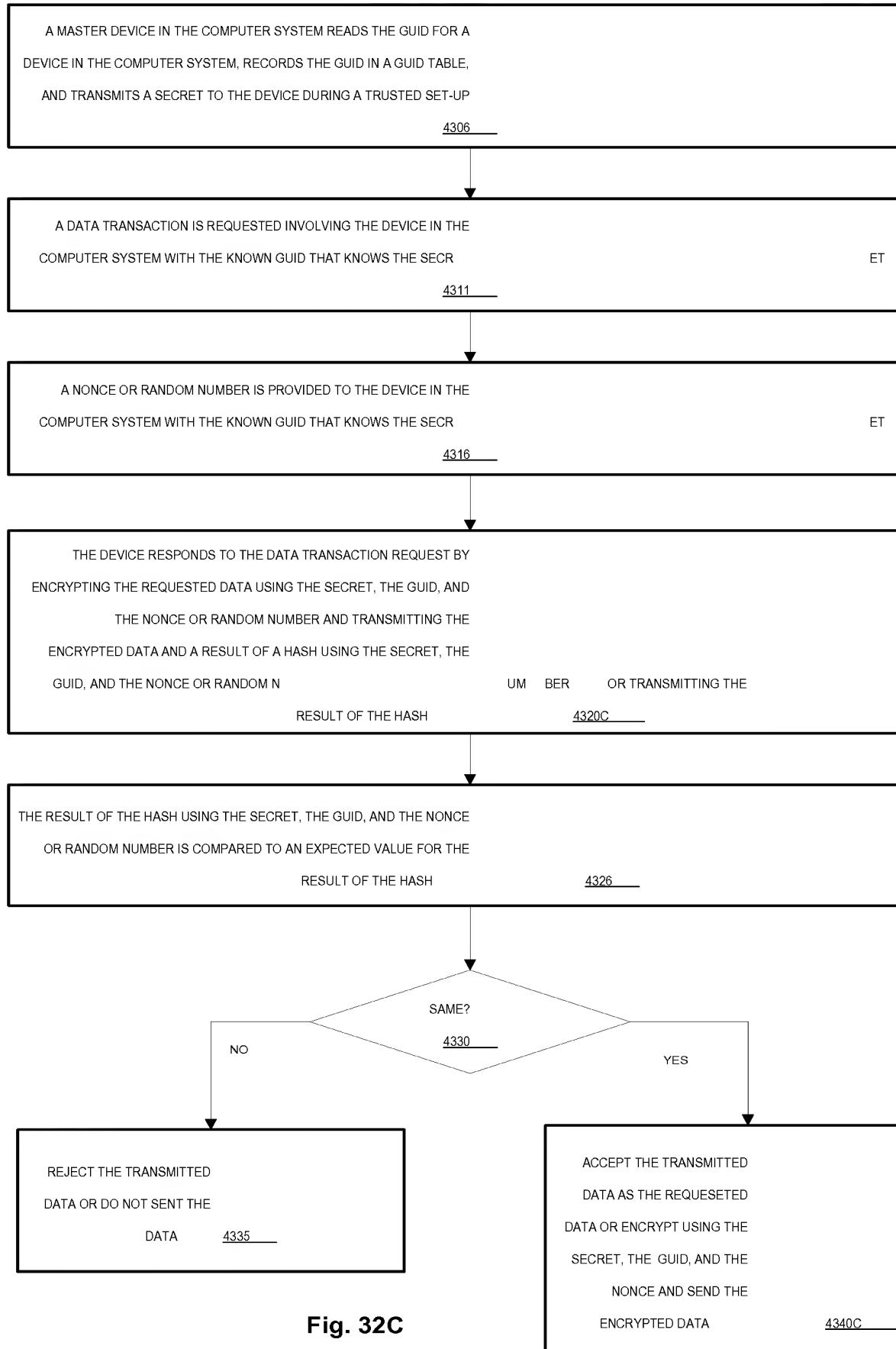


Fig. 32C

4300C

ET

ET

SMITTING THE

YES

TRANSMITTED
REQUESEED
PT USING THE
GUID, AND THE
AND SEND THE
ED DATA

4340C

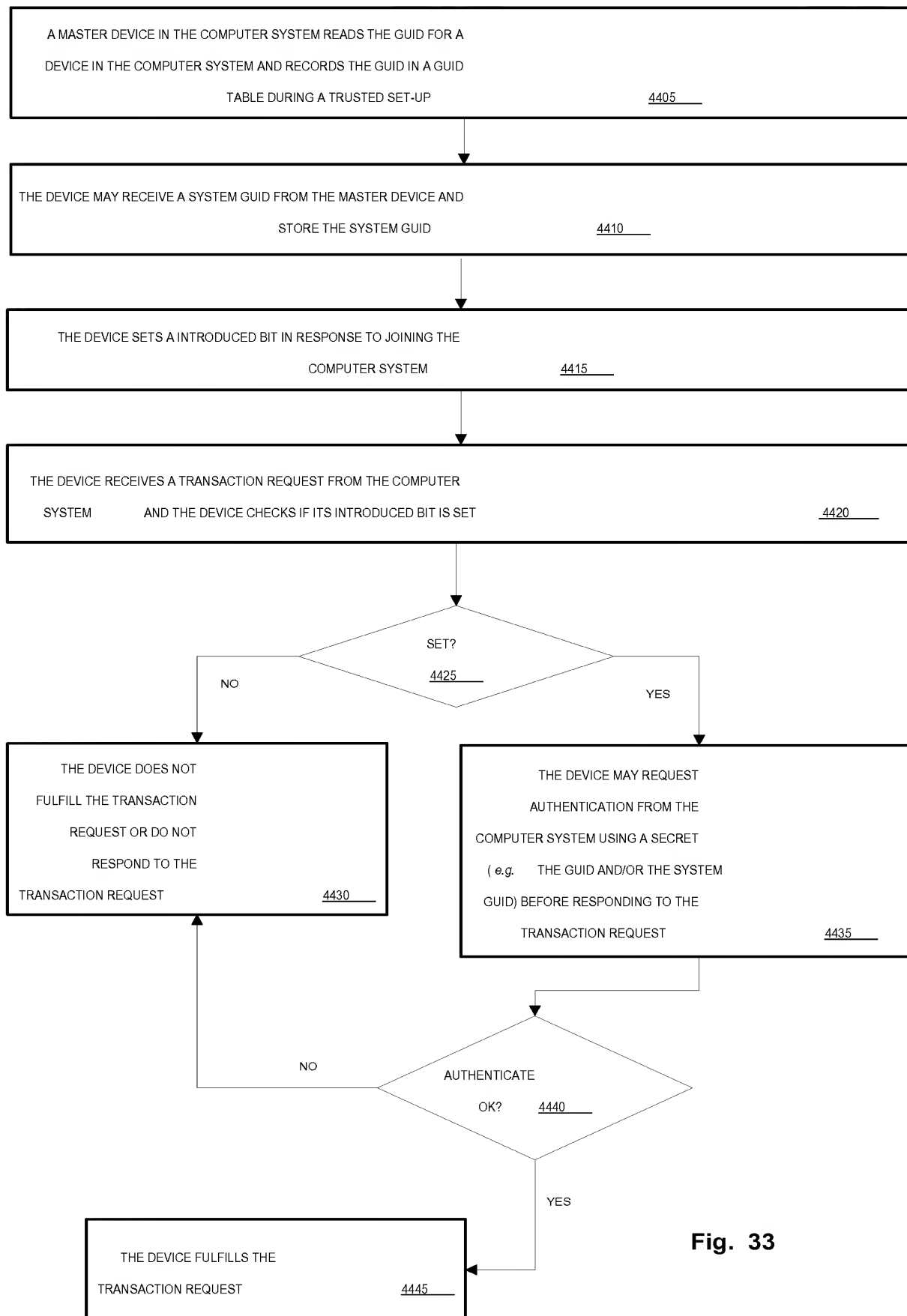


Fig. 33

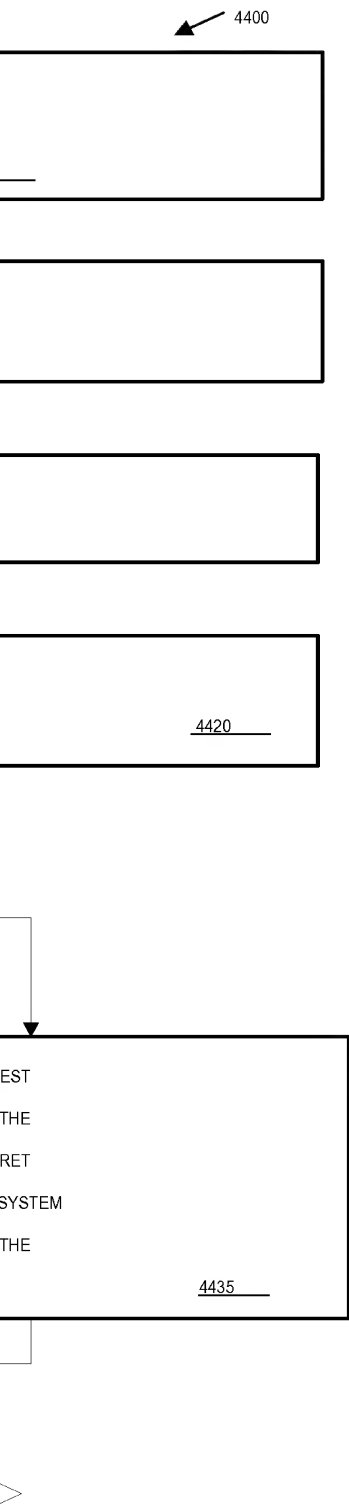


Fig. 33

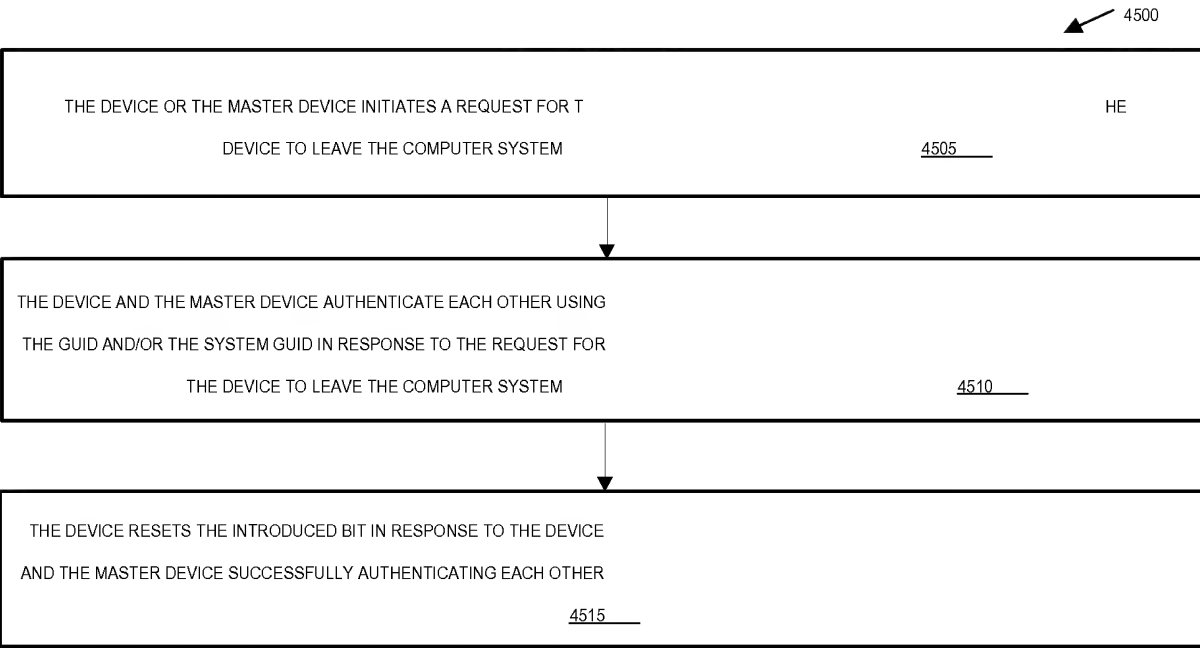


Fig. 34

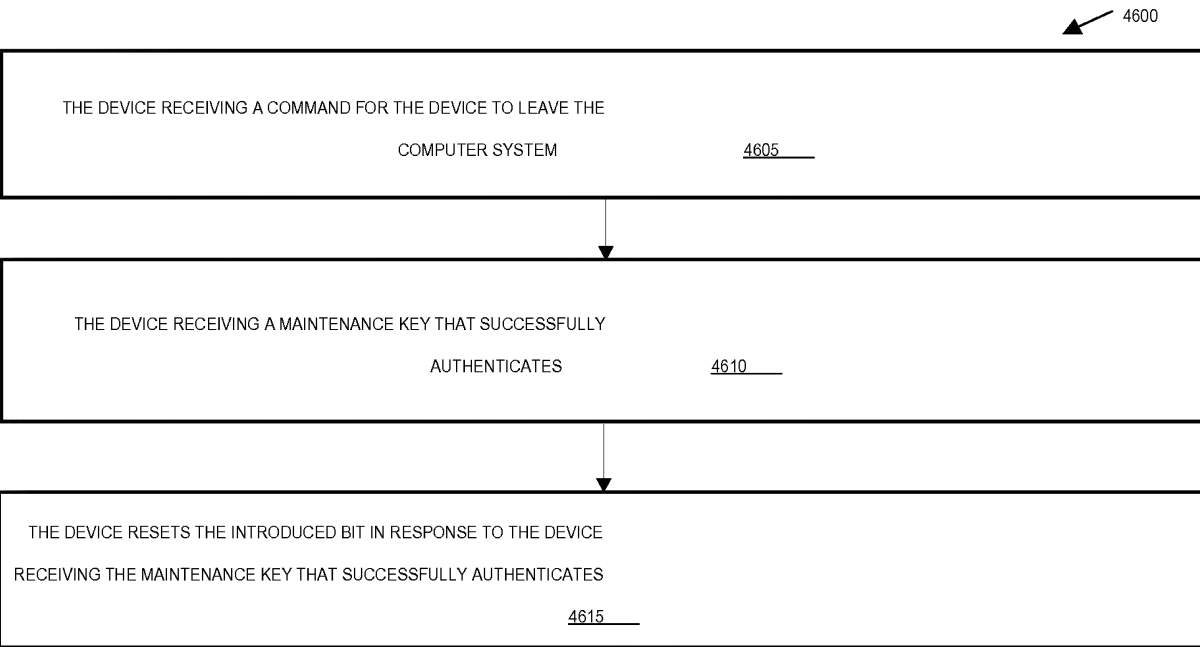


Fig. 35

4500

HE

4505

4510

4600

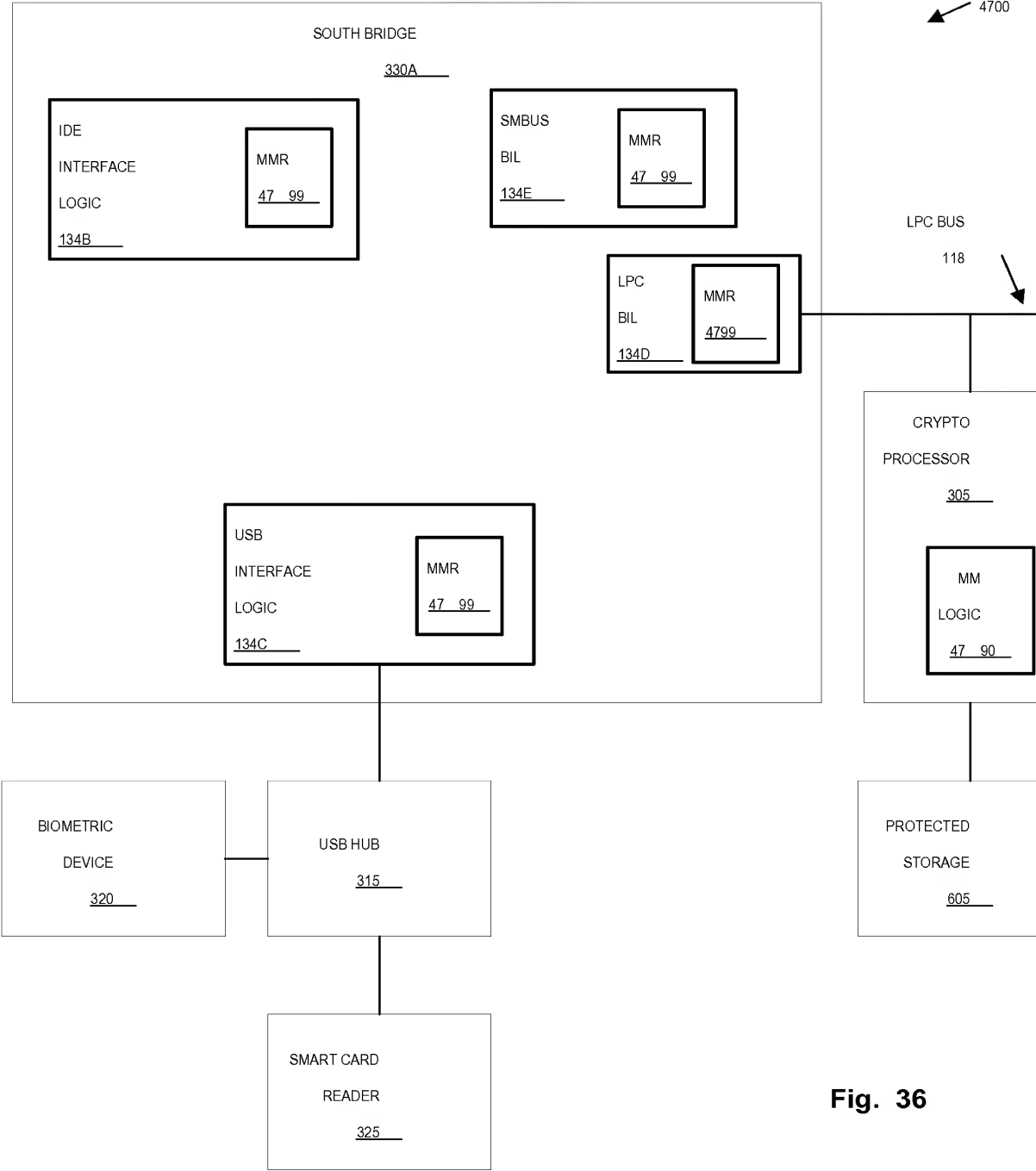


Fig. 36

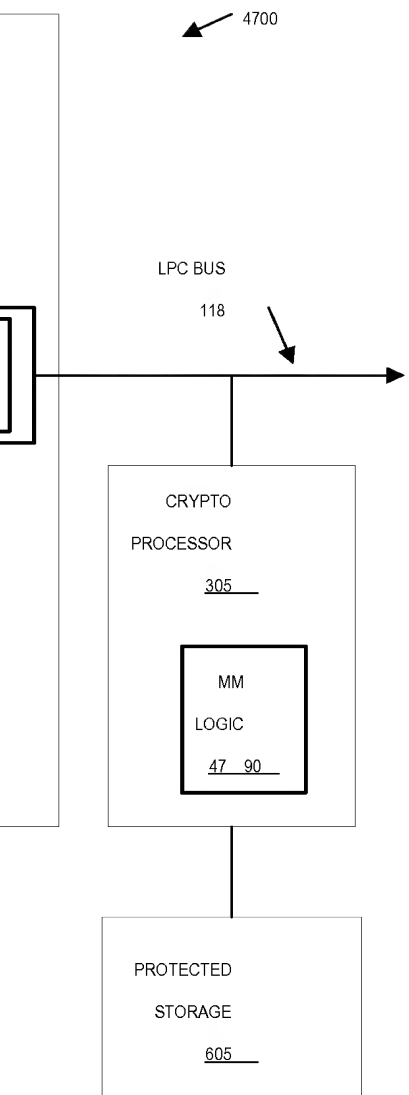


Fig. 36

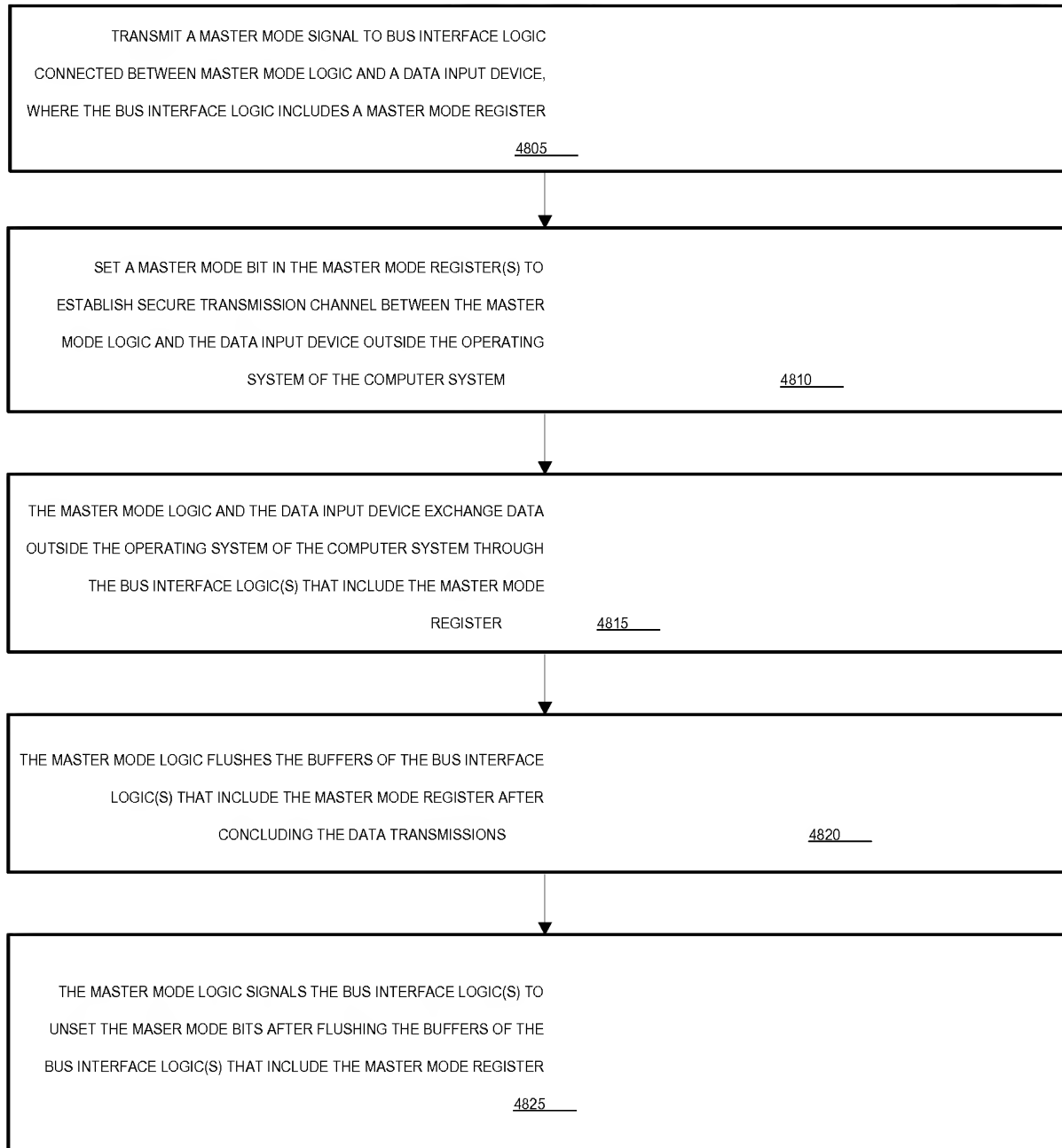


Fig. 37

4800



810

4820

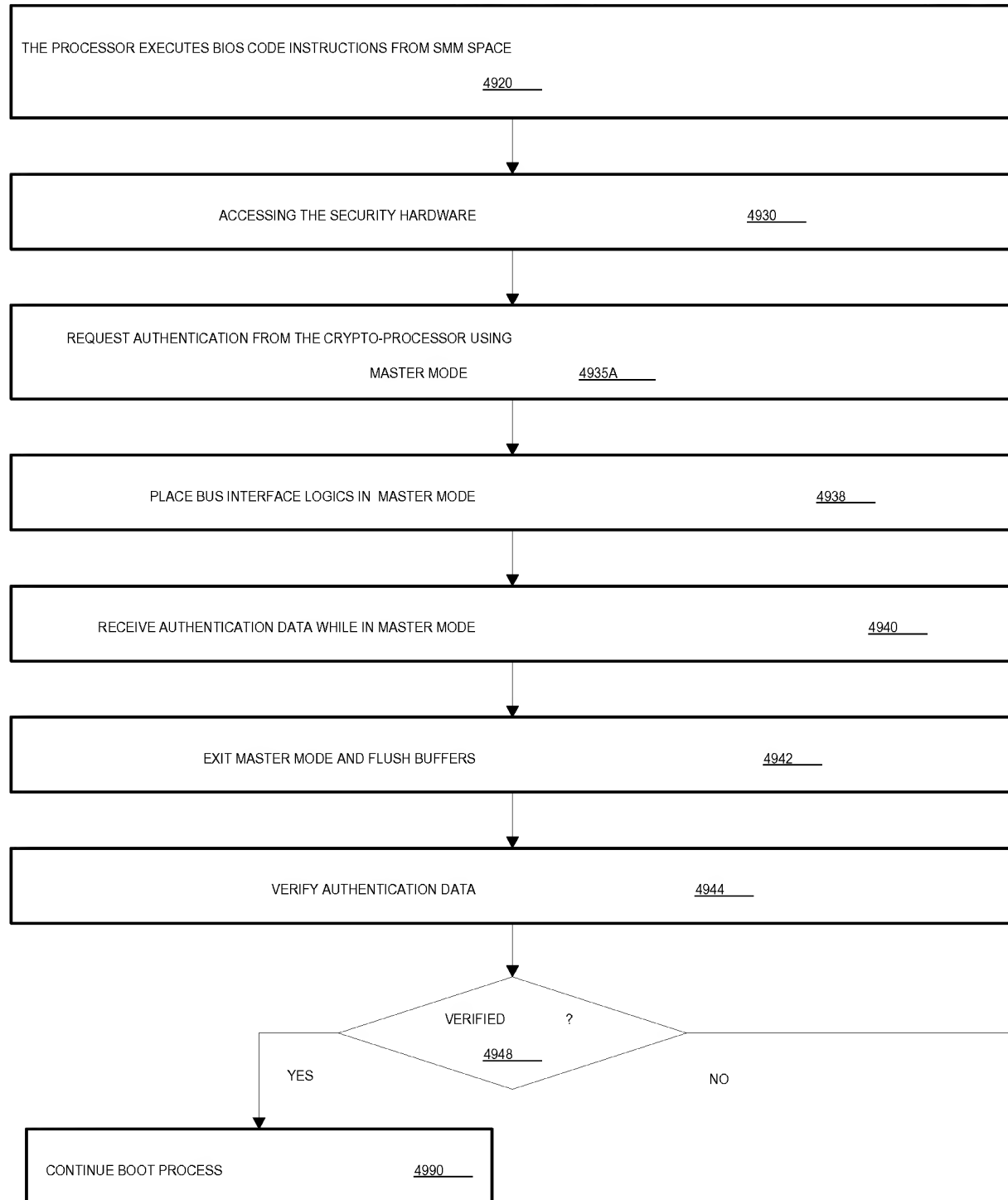


Fig. 3 8A

4900A

0

4938

4940

942



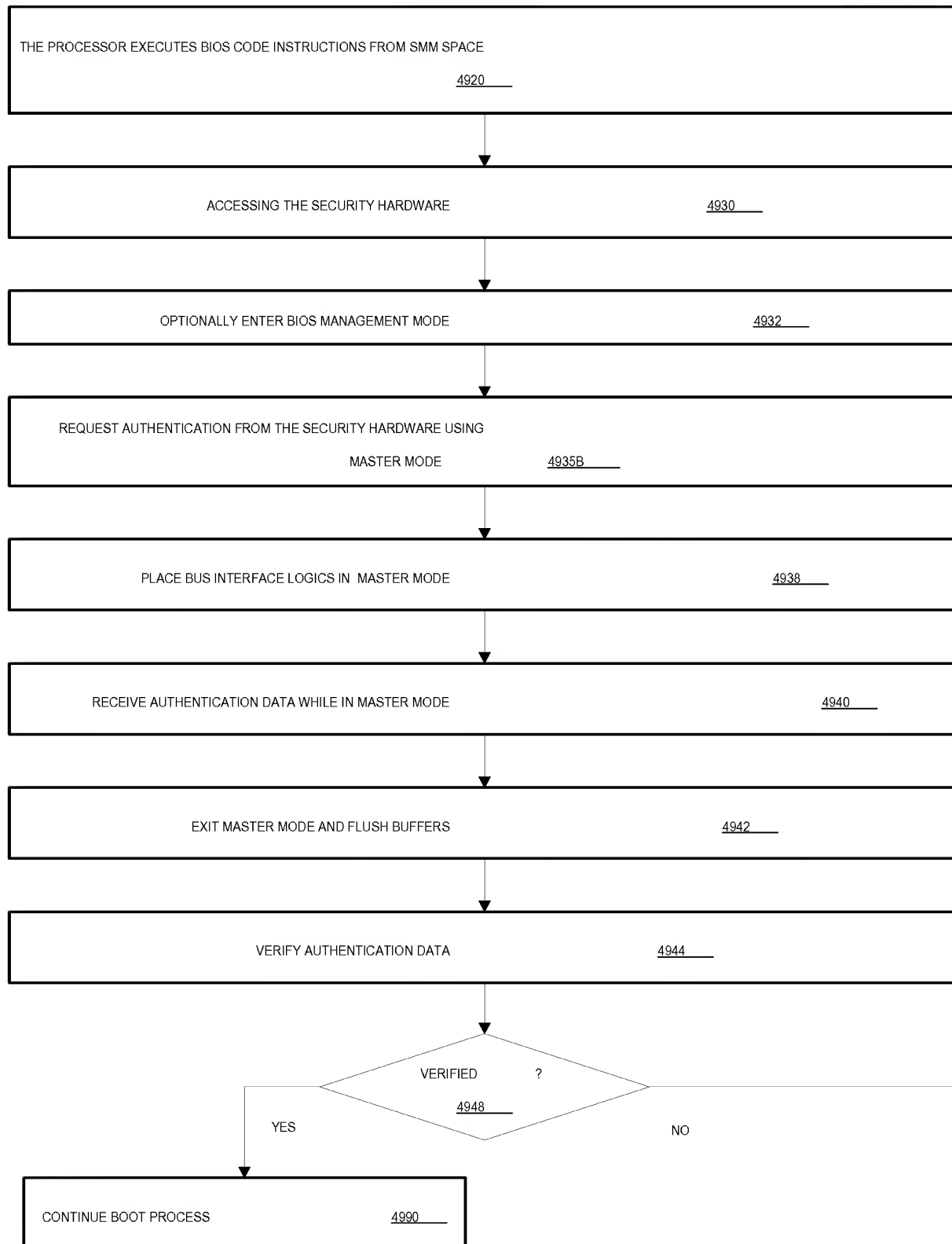


Fig. 3 8B

4900B

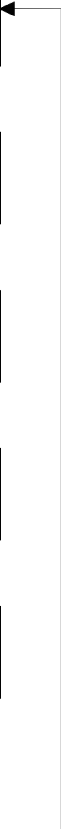
4930

4932

4938

4940

4942



5000A

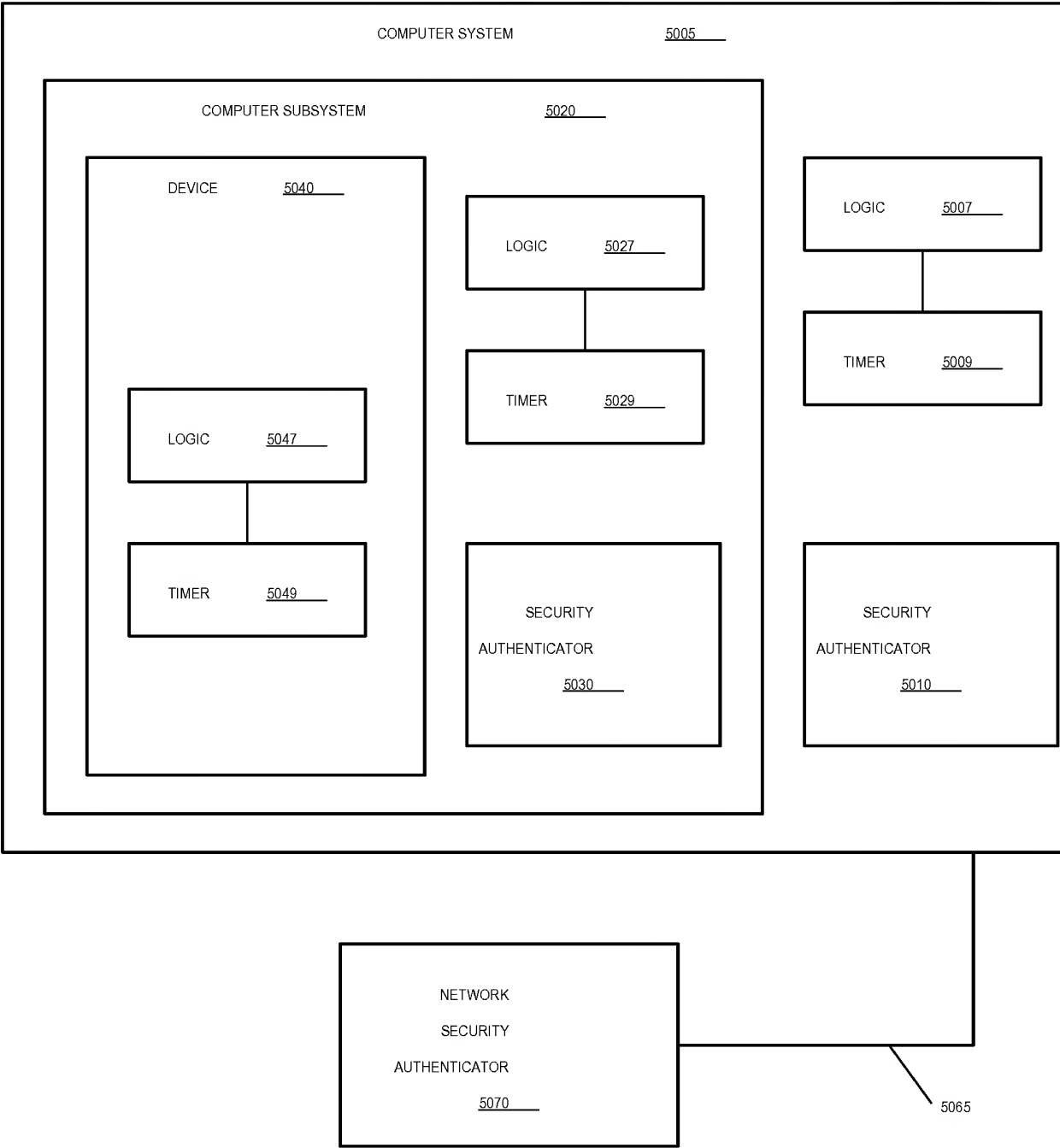
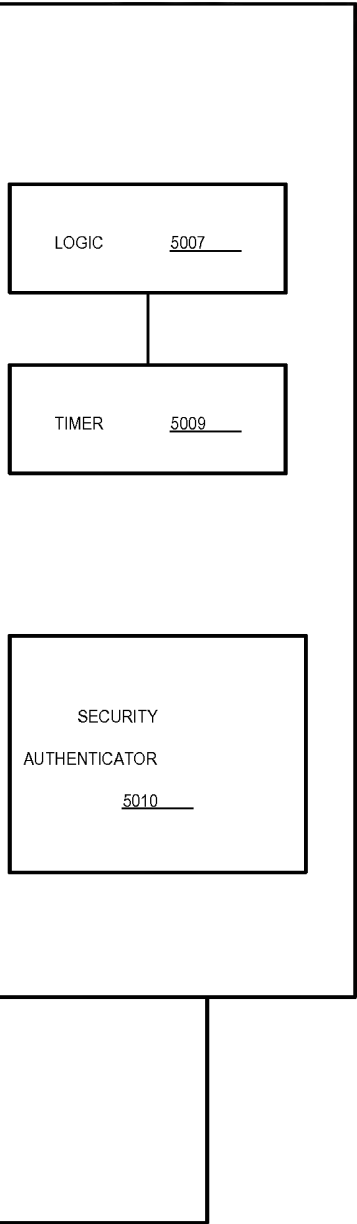


Fig. 39A

5000A



LOGIC 5007

TIMER 5009

SECURITY
AUTHENTICATOR
5010

5065

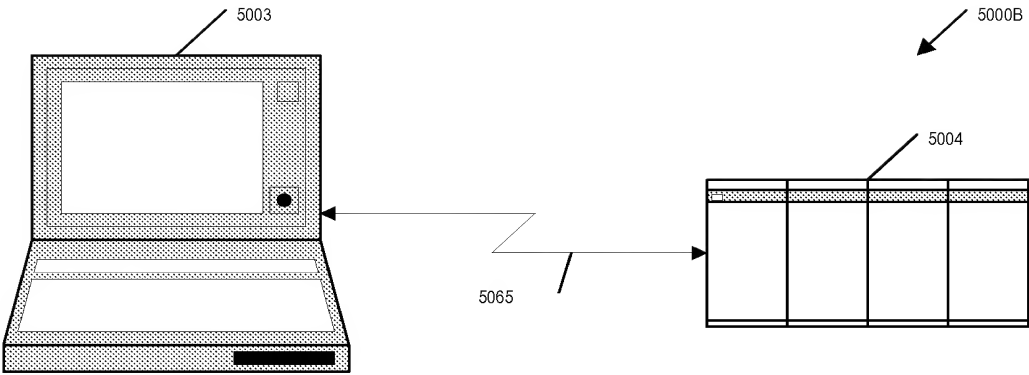


Fig. 39B

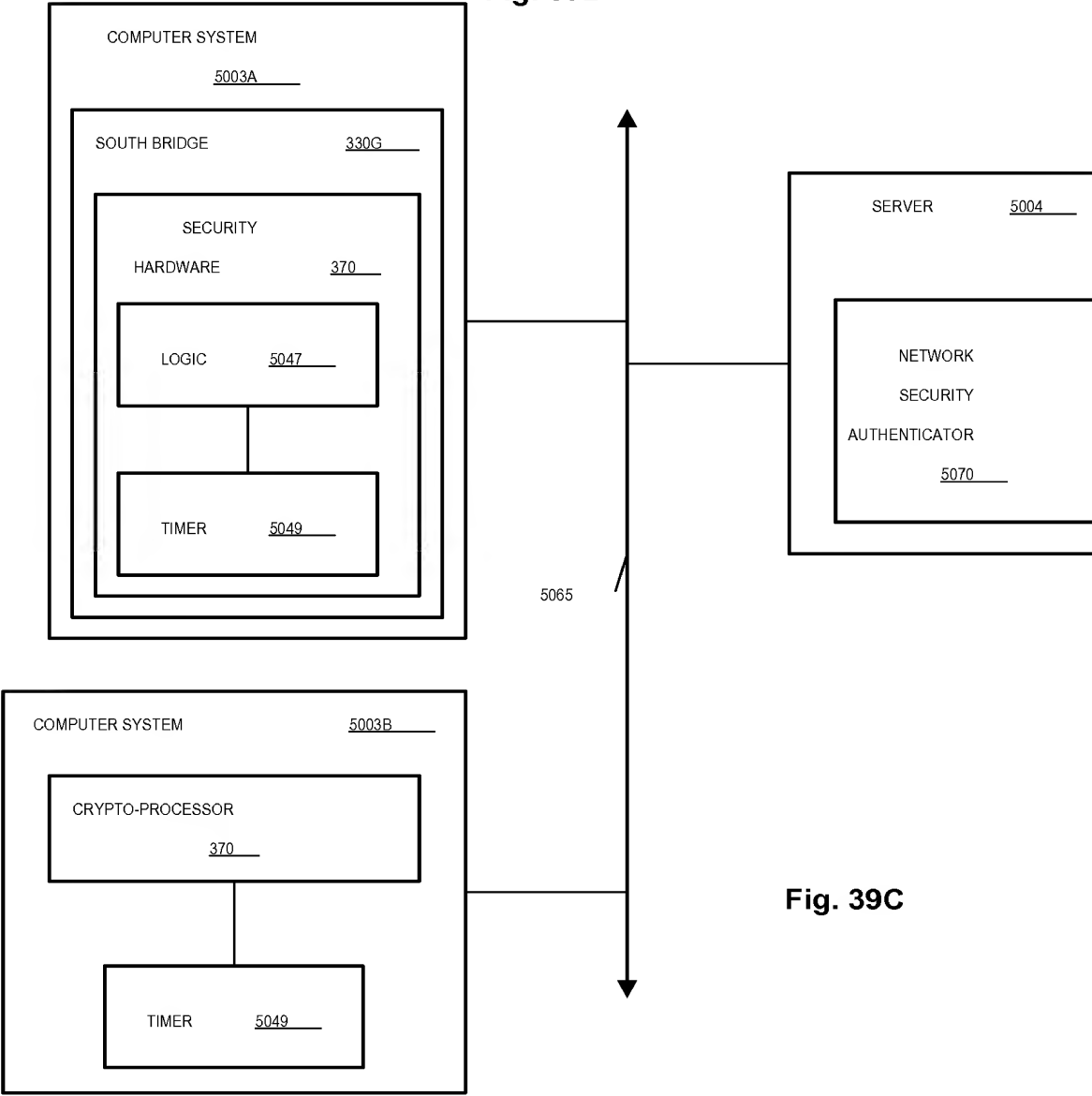
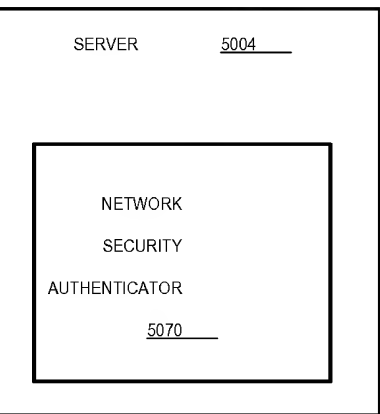
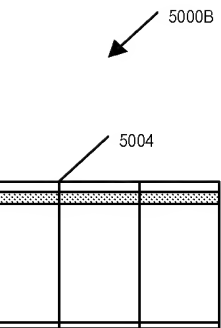


Fig. 39C



ig. 39C

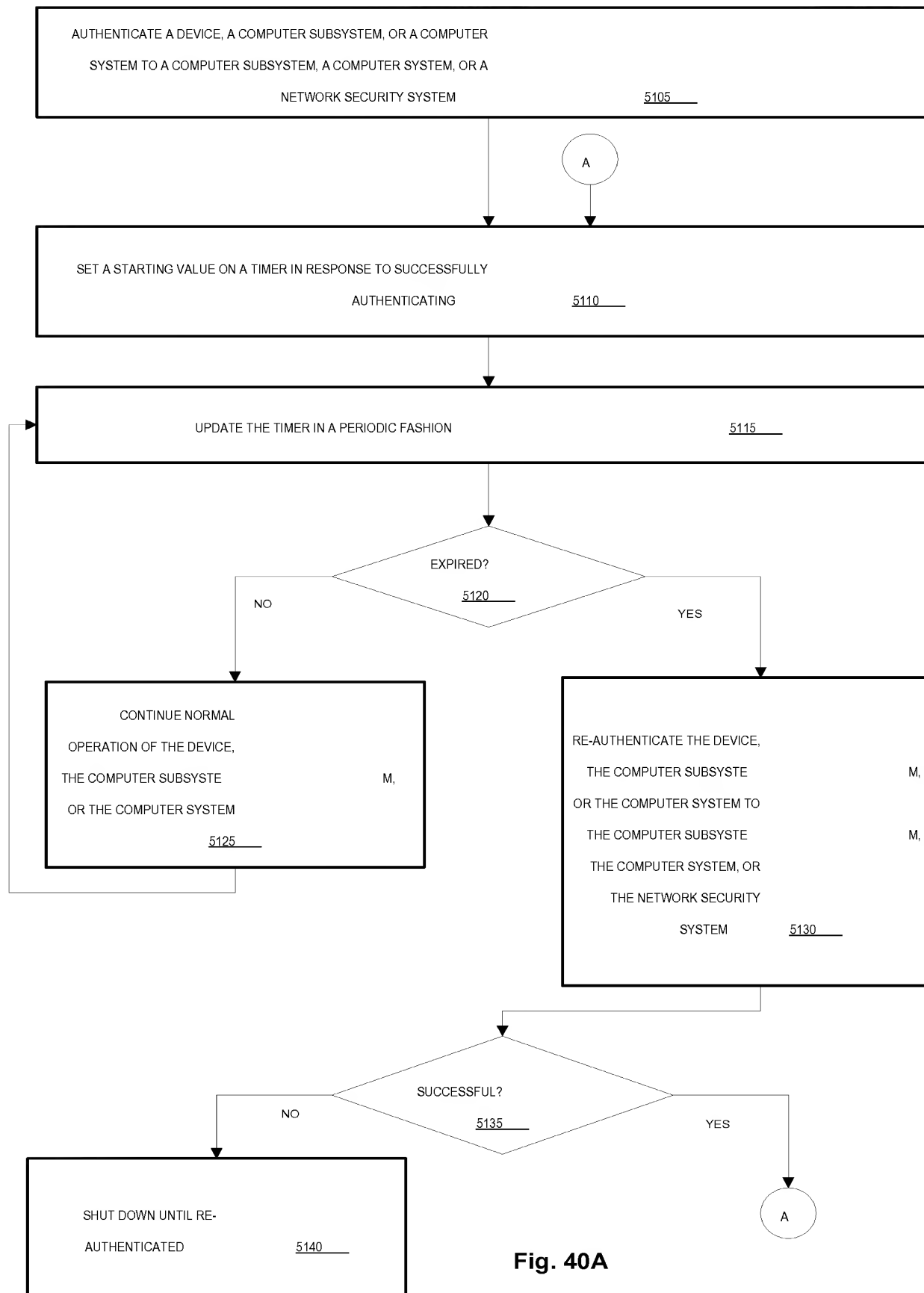
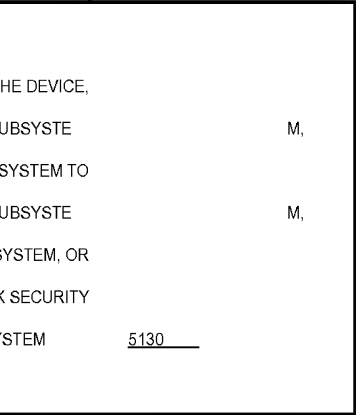
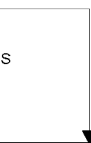
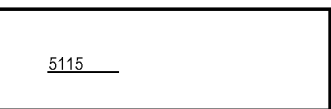


Fig. 40A

5100A



YES



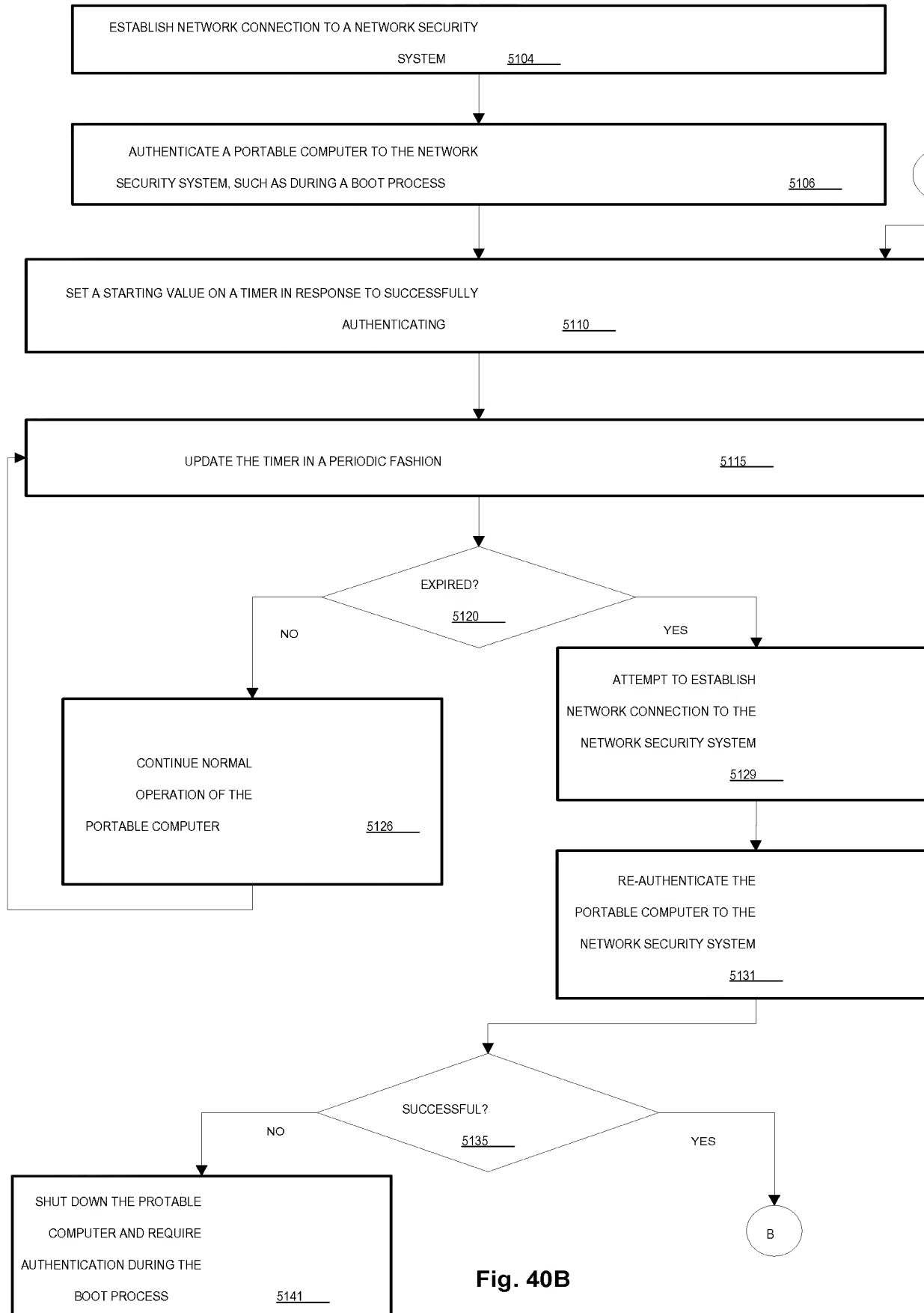
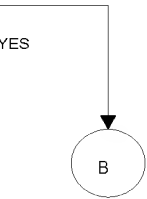
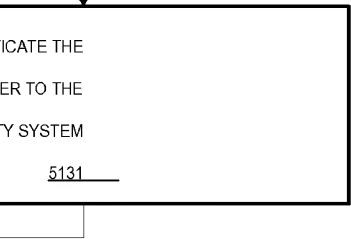
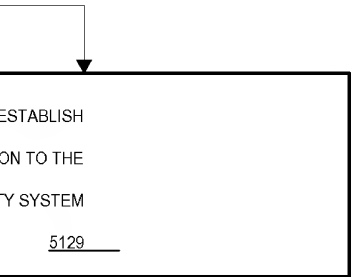
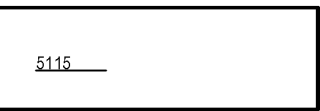
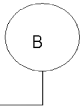
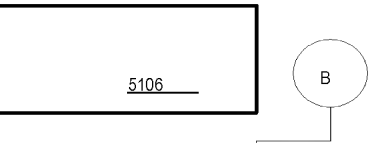
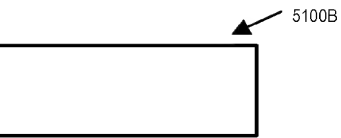


Fig. 40B



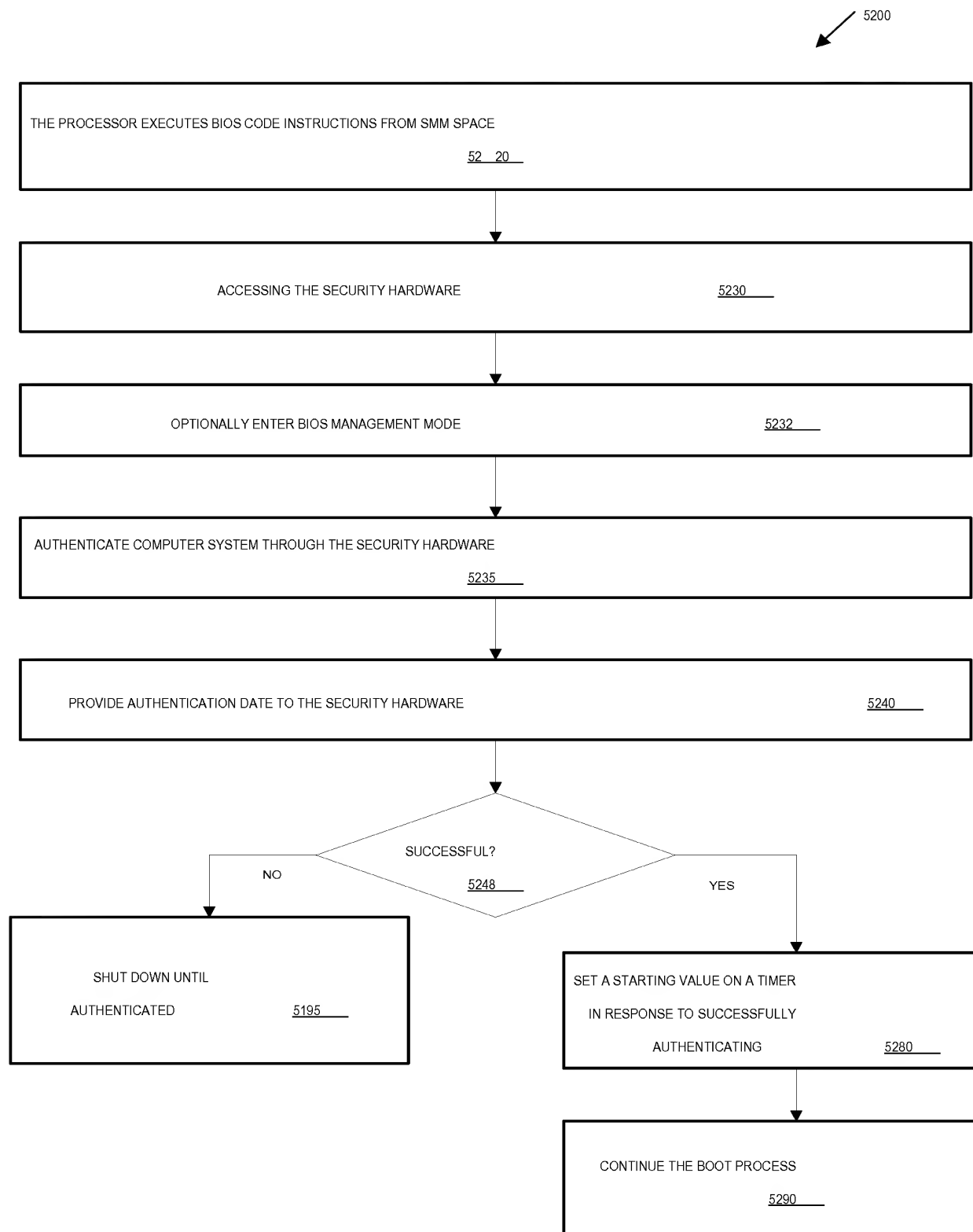


Fig. 41

5200

30

5232

5240

S

ON A TIMER

CESSFULLY

TING

5280

PROCESS

5290

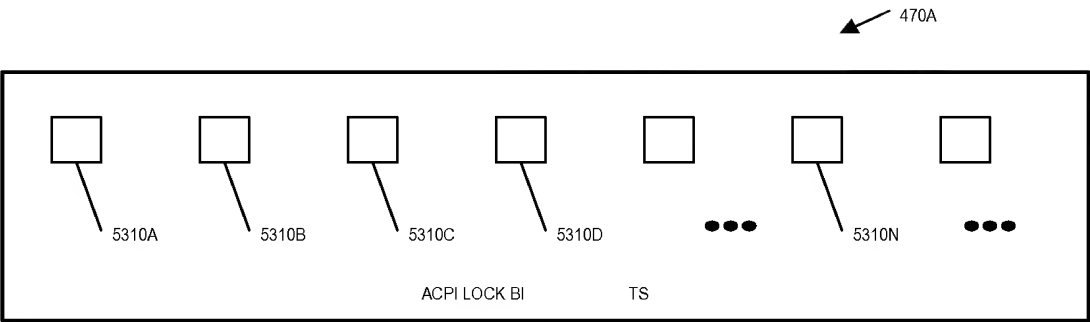


Fig. 42A

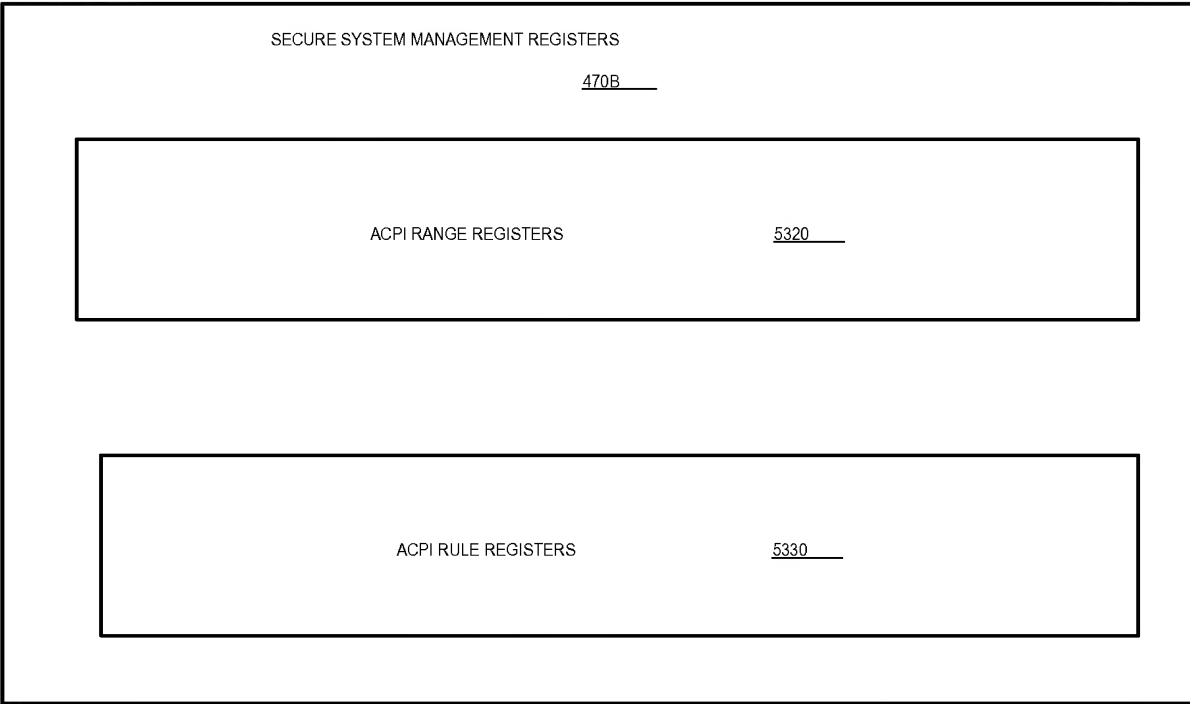


Fig. 42B

✓ 470A

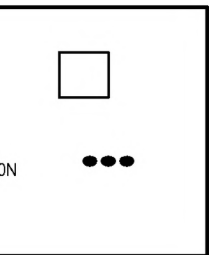


Fig. 42A

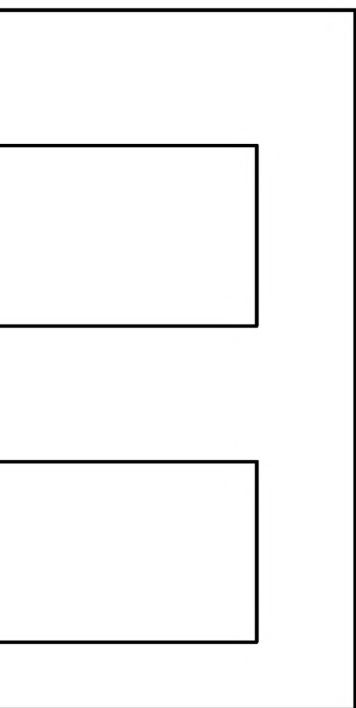


Fig. 42B